

PERFORMANCE WORK STATEMENT

In Support Of

CLIENT AGENCY:

**United States Department of Agriculture (USDA)
National Information Technology Center (NITC)**

PROJECT TITLE:

Information Technology Support

Original Version dated December 18, 2014

Table of Contents

1.	BACKGROUND	- 4 -
2.	OBJECTIVE	- 4 -
3.	SCOPE	- 5 -
4.	APPLICABLE DOCUMENTS.....	- 5 -
4.1.	Applicable Regulations and Documents	- 5 -
5.	TASK REQUIREMENTS	- 6 -
5.1.	Contract Line Item Numbers (CLINs)	- 6 -
6.	PERSONNEL	- 7 -
6.1.	General Requirements.....	- 7 -
6.2.	CLIN Specific Experience and Expertise	- 7 -
6.3.	Training.....	- 7 -
6.3.1.	Contractor Staff Training	- 7 -
6.3.2.	Seminars, Symposia, Or User Group Conferences	- 7 -
6.3.3.	Mandatory Government Training	- 7 -
6.4.	Personnel Retention and Recruitment.....	- 8 -
6.4.1.	Work Transition Plan.....	- 8 -
7.	QUALITY	- 8 -
7.1.	Quality Control	- 8 -
7.2.	Quality Assurance.....	- 9 -
8.	DELIVERABLES.....	- 9 -
8.1.	Contractor Submission.....	- 9 -
8.2.	Government Review	- 9 -
8.3.	Data and Deliverable Rights	- 9 -
8.4.	Transfer of Ownership	- 9 -
8.5.	Monthly Invoice.....	- 10 -
8.6.	Monthly Status Report	- 10 -
8.7.	Phase-In / Phase Out	- 10 -
8.7.1.	Phase-In Plan	- 10 -
8.7.2.	Phase Out Plan	- 11 -
8.8.	Deliverable Matrix	- 11 -
8.9.	Other Reporting Requirements	- 12 -
9.	PERFORMANCE	- 12 -
9.1.	General.....	- 12 -
9.2.	Kickoff Meeting.....	- 12 -
9.3.	Period of Performance	- 12 -
9.4.	Place of Performance	- 12 -
9.4.1.	Applicability of Telework.....	- 13 -
9.4.2.	Travel	- 14 -
9.5.	Hours of Work	- 14 -
9.5.1.	Standard Duty Hours Support.....	- 14 -
9.5.1.1.	Normal Workday - (work hour category A)	- 15 -
9.5.1.2.	Staggered Workday - (work hour category B).....	- 15 -
9.5.2.	Non-Standard Duty Hours Support.....	- 15 -
9.5.3.	Continuity of Operations (COOP)/Disaster Recovery (DR).....	- 15 -
9.5.4.	Holidays	- 16 -
9.5.5.	Government Administrative Leave Situations	- 16 -
10.	GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS	- 16 -

10.1.	General.....	- 16 -
10.2.	Property.....	- 16 -
10.2.1.	Facilities.....	- 16 -
10.2.2.	Equipment at Authorized On-Site Federal Work Locations	- 16 -
10.2.3.	Facilities and Equipment at Remote Work Locations.....	- 17 -
10.2.4.	Materials	- 17 -
10.2.5.	Validation of Government Furnished Items (GFI) and Equipment Inventory.....	- 17 -
10.3.	Use of Government Property	- 17 -
10.3.1.	Desk Telephones	- 17 -
10.3.2.	Mobile/Wireless Telephones and Smart Devices	- 17 -
10.3.3.	Mail/Postage	- 18 -
10.3.4.	Electronic Mail (E-mail)	- 18 -
10.3.5.	Copiers	- 18 -
10.3.6.	Fax Machines.....	- 18 -
10.3.7.	Computer and Internet	- 18 -
10.3.8.	Canvassing, Soliciting, or Selling	- 18 -
10.3.9.	Security Violations Using Government Equipment.....	- 18 -
10.4.	Government Vehicles.....	- 18 -
10.5.	Return of Government Property.....	- 18 -
10.6.	Conservation of Utilities	- 19 -
11.	SECURITY	- 19 -
11.1.	United States Citizenship.....	- 19 -
11.2.	Security Awareness Training	- 19 -
11.3.	Background Investigation Requirements	- 20 -
11.4.	Access to Sensitive/Critical Data.....	- 21 -
11.4.1.	Non-Disclosure Agreement.....	- 21 -
11.4.2.	Data Access.....	- 21 -
11.5.	Security Incident Reporting	- 21 -
11.6.	Permanent Security Badge Requirements.....	- 21 -
11.7.	Display of Permanent Security Badges.....	- 22 -
11.8.	Temporary Security Badge Requirements	- 22 -
11.9.	Facility Security Requirements.....	- 23 -
11.10.	Parking Requirements.....	- 24 -
12.	ADMINISTRATIVE CONSIDERATIONS.....	- 24 -
12.1.	Government Representatives	- 24 -
12.2.	Procedures for Payment	- 25 -
12.2.1.	Performance Based Payment Percentages	- 25 -
12.2.2.	Submission.....	- 25 -
12.2.3.	Non-Compliance	- 25 -
12.3.	Personal Service.....	- 25 -
12.4.	Section 508.....	- 25 -
12.5.	Privacy Act.....	- 25 -

PERFORMANCE WORK STATEMENT (PWS)

1. BACKGROUND

The National Information Technology Center (NITC) within the Office of the Chief Information Officer (OCIO) is charged with offering cost competitive, cloud-based, automated data processing hosting services to USDA and other federal government organizations. The NITC generates operating revenue under a “fee-for-service(s)” model administered through USDA’s working capital fund. NITC has grown in responsibility as the number of physical and virtual, mid-tier servers has grown based on customer demand. It is anticipated that the growth will continue. At the time of preparing this performance work statement, the NITC is supporting USDA customers and other federal government organizations as they strive to achieve the President’s mandate to dispose of unneeded federal real estate and consolidate federal data centers.

The NITC provides comprehensive, cloud-based hosting services, associated operations, security, and professional support services to a customer base of 35 federal organizations. The Enterprise Data Center hosts business applications supporting millions of citizens across the United States of America. The NITC organization has been designated a USDA Enterprise Data Center with locations in Kansas City, MO; St. Louis, Missouri; Beltsville, Maryland; Washington, DC; Salt Lake City, UT; Fort Worth, TX; and Fort Collins, CO. The NITC has earned the title of a GSA FedRamp certified cloud service provider.

The NITC utilizes an IT Infrastructure Library / IT Service Management (ITIL/ITSM)-based framework to develop processes & policies for all work activity tracking, process management and workflow. The current ITSM automation suite is provided through BMC’s Remedy COTS offering. The ITSM suite will generate task assignment queues. The policies and direction for many of these automated processes are directed by the Enterprise Change Control Board (ECCB) which governs the tool implementation. The contractor shall use this tool and adapt to the methods implemented by the NITC. During the course of this task order, the ITSM Remedy systems of the NITC and International Technology Services (ITS) organizations will continue to data share to provide unified responsiveness. It is anticipated that data sharing and ticket assignment will continue to be enhanced in the coming years.

The NITC also partners with the ITS to provide hosting and network solutions for USDA’s Service Center Agencies (i.e., Farm Service Agency, Natural Resources and Conservation Service and Rural Development). This task order seeks to continue to improve those services that are provided through the use of Memorandum of Understandings (MOUs), Service Level Agreements (SLAs) and Operating Level Agreements (OLAs). The contractor shall to adhere to the language and conditions of these documents. Copies of all MOUs/SLAs/OLAs relevant to this task order that are in place at the time of award will be provided to the contractor. The MOUs/SLAs/OLAs facilitate the understanding of the separate but shared roles and responsibilities for services that are provided by the OCIO organizations.

2. OBJECTIVE

The objective of this task order is to provide Information Technology (IT) support services to complement in-house capabilities in order to meet the short and long-range plans of both USDA and non-USDA serviced agencies. Specific objectives include, but are not limited to, those identified below.

- **Objective 1** - The Contractor shall work as a part of the technical support team that the NITC leverages to provide world-class data center service offerings and professional services to the USDA and other federal government customers (i.e., customer base) and shall enable the increased visibility of NITC value-added benefits by meeting or exceeding service expectations. In the data center operational support context, the support team is comprised of vendor-dispatched hardware maintenance personnel; vendor specific hardware and software technical “hot-line” support personnel; federal employees, and contractor employees. Given the complexity of the data center hosting environment and the customer base’s application software systems running on the hosting environment, system outages could require all or some of the support team, described above, to be mobilized to resolve the emergency.
- **Objective 2** - The Contractor shall support NITC data center officials in the completion of task assignments securing the availability, reliability and integrity of the data center through routine

operations & maintenance activities.

- **Objective 3** - The Contractor shall support NITC data center officials in the completion of work order priorities assigned through the ticketing system (i.e., NITC's implementation of BMC's Remedy COTS) and defined by the NITC Incident Management Process Guide. The contractor shall support incident, change and problem management and shall reinforce incident coordination and service metric tracking to staff.
- **Objective 4** - The Contractor shall support NITC data center officials in the preparation of documentation for the NITC Change Control Board.
- **Objective 5** - The Contractor shall support NITC data center officials with the implementation of federal mandates and the seam-less coordination with other OCIO organizational units.
- **Objective 6** - The Contractor shall support NITC data center officials with a full range of back office functions for the budgetary, financial and administrative management of the center.
- **Objective 7** - The contractor shall ensure close coordination, communication, and resource sharing and shall support resolution, restoration, and root cause analysis to reduce mean time to repair and reduce the overall cost of operations and maintenance support.
- **Objective 8** - The contractor shall support the achievement of long-term cost reduction by adapting ITIL best practices and applying automation to data center operations that reduce overall costs and better allocate resources.

3. SCOPE

The projects of the data center are national in scope and impact the United States economy. The scope of work for this PWS will cover a full range of functional areas and technical skill sets required to support the USDA, OCIO, NITC. The task order may include, but not be limited to, the IT support services for work to be accomplished using different computing environments that can include various hardware platforms, software, and telecommunications capabilities currently installed or planned to be installed by the NITC or customer agencies. This will require qualified personnel with expertise in computer equipment, software, and telecommunications facilities used in customer agency offices. The skill sets needed will vary depending upon the requirements.

USDA agencies are currently using, but are not limited to, the following types of hardware and software:

- NITC hardware and software include installed IBM-compatible mainframe computers, z/OS operating system with JES2 and VTAM, TSO, CICS, FOCUS, IDMS, and DB2.
- Other equipment currently in use includes SUN, HP, RISC based systems, and IBM-compatible PCs.
- Software currently in use includes ORACLE, S2K, SYBASE, C, SAS, COBOL, FORTRAN, UNIX, WINDOWS (200X), INFORMIX, DB2, Cold Fusion, Java, MS SQL, Adobe Acrobat, Adobe Photoshop, and Web Trends and other Web development tools, including WebSphere.

NITC supports multiple mainframe systems, several thousand mid-range systems, and various storage platforms. The current system environment includes: IBM, Sun, HP, and Intel-based servers with LINUX, AIX, Unix, HP-UX, Sun Solaris, Windows (9X, NT, and 200x), and Windows Data Center Operating systems, and storage solutions including Storage Area Networks. NITC offers multi-platform application, database support, and maintenance. Some of these include: High Availability Solutions, Mail/Directory Server Applications, Web Servers, and Database Applications.

NOTE: The above information is for general reference and subject to change. The IT environments at the NITC and customer agencies are dynamic and can change constantly.

4. APPLICABLE DOCUMENTS

4.1. Applicable Regulations and Documents

The following documents (versions current at time of award) are incorporated into the resultant task order award. Succeeding revisions may be substituted or incorporated as required. This list is not all inclusive and or limited to the following:

- http://wiki.edc.usda.gov/mediawiki/index.php/Main_Page.
- ACM-0015-01 - Human Resources Management Contractor In-Process Rev 2 (PWS Attachment D-1).
- ACM-0015-02 - Human Resources Management Contractor Exit Process Rev 2 (PWS Attachment D-2).
- Applicable NITC Directives that will be released after the resultant task order award.

5. TASK REQUIREMENTS

The contractor shall furnish all personnel, services, and supervision to perform the requirements of this task order. The contractor shall provide facilities and equipment for back office administration. Contractor employees shall clearly identify themselves as such at all times (badge display; identification announcement prior to or at the commencement of meetings and teleconferences; and correspondence including e-mail, etc.)

5.1. Contract Line Item Numbers (CLINs)

The specific task requirements to be completed under the below identified CLINs are included in PWS Attachment A, which includes the performance standards for the firm fixed price (FFP) CLINs. Additional performance standards for the labor hour (LH) CLINs are included in PWS Attachment B. Additional CLIN specific requirement information, presented in a summary display, is identified in PWS Attachment C.

CLIN Number	CLIN Title	CLIN Type
001	Audit Support Services	FFP
002	Budget Analysis Support Services	FFP
003	Business Continuity Planning Services	FFP
004	Enterprise IT Services Portfolio Management	FFP
005	Facilities Operations Services	FFP
006	Information Systems Security Support Services	FFP
007	ITSM Process Development and Documentation Services	FFP
008	ITSM Service Asset and Configuration Management Support Services	FFP
009	Program/Project Management Review Support Services	FFP
010	Task Order Management	FFP
011	Technical Architecture Support Services	FFP
012	Technical Writer	FFP
013	ADDM Administration & Modeling Services	LH
014	Application Integration Engineering Support Services	LH
015	Data Center Hardware Support Services	LH
016	Database Administration Services	LH
017	Mainframe Systems Programming Services	LH
018	Network Engineering Services	LH
019	Remedy Engineering and Administration Services	LH
020	Security Administration Services - AD & Identity Management	LH
021	Security Administration Services - MF Auth., Role Mgmt. & Access Cont.	LH
022	Security Engineering - Assessment Services	LH
023	Security Engineering - Monitoring, Detecting & Analysis Services	LH
024	Security Engineering - Network Access Control Services	LH
025	Senior Application Engineering Services	LH
026	Server Automation Tool Support Services	LH
027	Storage Administration Services	LH
028	Systems Administration Services	LH
029	Systems Monitoring Administration Services	LH

6. PERSONNEL

6.1. General Requirements

All contractor employees shall meet the minimum general requirements listed below.

- Strong written and oral communication skills in the English language. All contractor employees must be able to read, write, speak and understand English.
- Contractor personnel performing in a leadership capacity shall be capable of directing contractor personnel and interfacing with the Government and customers.
- Exceptional customer service skills.
- Strong time-management and prioritization skills.
- Ability to communicate applicable technical subject matter expertise to management and others.
- NITC follows the IT Infrastructure Library (ITIL) service operation best practices. It is important for the employees to demonstrate experience based on ITIL framework:
 - ITIL v3 foundation knowledge (or certification).
 - Ability to apply and provide feedback on service operation model and practices.

6.2. CLIN Specific Experience and Expertise

Documented experience and ability to demonstrate knowledge/skills/abilities with the required items (i.e. technologies, organizations, systems, processes, etc.) listed in the CLIN descriptions is required.

6.3. Training

6.3.1. Contractor Staff Training

The Contractor shall provide fully trained and experienced support staff for performance of the task order. Training of contractor personnel shall be performed at the Contractor's expense, except when the Government changes the requirements during performance of an on-going task and it is determined to be in the best interest of the Government. This will be negotiated on a case-by-case basis. Training at Government expense will not be authorized for replacement personnel nor for the purpose of keeping Contractor personnel abreast of advances in the state-of-the-art, or for training Contractor employees on equipment, computer languages, and computer operating systems that are available in the commercial market.

6.3.2. Seminars, Symposia, Or User Group Conferences

The Government will not authorize training for contractor employees to attend seminars, symposia, or User Group Conferences unless certified by the Contractor that attendance is mandatory for the performance of the task order requirement. When seminars, symposiums or User Group Conferences are authorized in writing by the COR, the Government will reimburse the Contractor for labor hours. The Contractor shall be responsible for expenses associated with the training, including, but not limited to, tuition, travel and per diem. This will be negotiated on a case-by-case basis

6.3.3. Mandatory Government Training

Mandatory Government training shall be tracked and monitored through USDA's AgLearn system. A new contractor employee must complete security training before a log-on ID to USDA systems is issued. The contractor shall provide the information to the employee to review. The contractor will then proctor an exam that the contractor employee will complete and provide to the NITC COR. The NITC COR submits the exam to the NITC Federal Training Coordinator for exam grading. Once the contract employee passes the test they will be granted access to USDA systems, including AgLearn. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position. Each contractor employee must complete annual training classes as mandated by USDA. The current mandatory courses include Security Awareness, Privacy Basics, and some positions require Role-Based Security training. These mandatory AgLearn courses can be completed through the AgLearn website free-of-charge. The COR shall notify the

contractor of the training requirements and will provide the tools to complete this training. All required courses must be completed by the required dates by all contract employees. Mandatory government training classes may be completed during work hours. It is the intent of USDA to provide 30 calendar days written notice of annual training requirements to the Contractor's Task Order Manager. The Task Order Manager will be responsible for notifying subordinate contractor employees. In the event the contractor does not receive 30 calendar day notice, the contractor is still required to complete the training by the specified date(s).

6.4. Personnel Retention and Recruitment

The Contractor shall make every effort to retain personnel in order to ensure continuity until contract completion. If it should become necessary to substitute or replace personnel, the Contractor shall immediately notify the COR in writing of any potential vacancies and shall submit the resume(s) of replacement personnel within 14 calendar days of the notification. Additionally, for all new positions identified by the Government, the Contractor shall submit the resume(s) of proposed personnel within 14 calendar days of the Government's initial request. The Contractor shall submit the resume(s) of all potential personnel selected to perform under this task order to the COR through Information Technology Solutions Shop (ITSS) for Government review and acceptance/rejection. Upon Government acceptance of a personnel resume(s), the candidate shall be available to begin performance within 14 calendar days. The contractor shall ensure continuity of operations during periods of personnel turnover and long-term absences. Long-term absences are considered those longer than one week in duration.

6.4.1. Work Transition Plan

Due to the technical nature of the work and "least privilege" security access of user accounts, a situation could arise where work must be transitioned back to Government personnel upon a contract employee's departure from the workforce. In this situation, the contractor shall provide documentation in sufficient detail to allow for the transition of the workload to the Government. The Contractor shall provide documented processes that will serve as a basis for knowledge transfer and a historical record of the work accomplished. Documentation shall include a summary report on task requirements, contact information, and the location of documentation needed to provide continuity of service. This documentation must allow the Government to perform all tasks without the assistance of the Contractor.

7. QUALITY

Both the contractor and Government have responsibilities for providing and ensuring quality services, respectively.

7.1. Quality Control

The contractor shall establish and maintain a complete Quality Control Plan (QCP) to ensure the requirements of this contract are provided as specified in accordance with the applicable Inspection of Services Clause. The CO will notify the contractor of acceptance or required modifications to the plan. The contractor shall make appropriate modifications (at no additional costs to the government) and obtain acceptance of the plan by the CO. The Government has the right to require revisions of the QCP (at no cost to the Government) should the incorporated plan fail to deliver the quality of the services provided at any time during the contract performance. The plan shall include, but is not limited to the following:

- A description of the inspection system covering all services listed.
- The specification of inspection frequency.
- The title of the individual(s) who shall perform the inspection and their organizational placement.
- A description of the methods for identifying, correcting, and preventing defects in the quality of service performed before the level becomes unacceptable.

On-site records of all inspections conducted by the Contractor are required. The format of the inspection record shall include, but is not limited to, the following:

- Date, time, and location of the inspection.
- A signature block for the person who performed the inspection.
- Rating of acceptable or unacceptable.
- Area designated for deficiencies noted and corrective action taken.
- Total number of inspections.

7.2. Quality Assurance

The Government will perform periodic reviews of the contractor's performance in accordance with the Government's Quality Assurance Surveillance Plan (QASP). The Government reserves the right to review services to be provided, including those developed or performed at the Contractor's facilities, to determine conformity with performance and technical requirements. Government quality assurance will be conducted on behalf of the CO. The COR will be appointed to coordinate the overall quality assurance of technical compliance.

8. DELIVERABLES

Deliverables and due dates are identified in subsequent paragraphs.

8.1. Contractor Submission

Deliverables are to be transmitted with a cover letter, on the prime contractor's letterhead, describing the contents, electronically through GSA's web-based procurement system, ITSS, and to any other destination(s) as required per the Government's request. The contractor shall provide hard copy deliverables as required per the Government's request. All deliverables shall be produced using recommended software tools/versions as approved by the Government. All reports shall be accomplished utilizing the MS Office Software Suite to include MS Project as required.

8.2. Government Review

Government personnel will have 10 workdays to review deliverables (to include resubmissions) and provide written acceptance/rejection. The NITC USDA client representatives and/or the applicable COR(s) will notify the contractor of deliverable acceptance or provide comments in writing. The contractor shall incorporate Government comments, or provide rationale for not doing so within 5 days of receipt of comments. Government acceptance of the final deliverable will be based on resolution of Government comments or acceptance of rationale for non-inclusion. Additional changes volunteered by the contractor will be considered a resubmission of the deliverable.

8.3. Data and Deliverable Rights

All information such as software, data, designs, test materials, documents, documentation, notes, records, software tools acquired, and/or software source code and modifications produced by the contractor under this PWS shall become the sole property of the U.S. Government, which shall have unlimited rights to all materials and determine the scope of publication and distribution. The contractor shall be required to deliver electronic copies of all documents, notes, records and software to the Government upon termination of the task order or expiration of the task order. The Government shall retain ownership of all proprietary information and intellectual property generated under this task order.

8.4. Transfer of Ownership

All data and documentation, including all studies, reports, spreadsheets, software, data, designs, presentations, documentation, etc., produced by the contractor or for the Government using this PWS are the property of the Government upon its taking possession of task deliverables or upon termination of the task order or expiration of the task order.

8.5. Monthly Invoice

The contractor shall provide a monthly invoice to be submitted simultaneously with the monthly status report. Both documents shall be provided to applicable parties. The invoice and monthly status report shall be submitted as a single file. The components of the single file shall be arranged in the following order: accounting format invoice, monthly status report, and additional documentation as required.

The invoice shall include but not be limited to:

- Labor hours expended. The labor hours expenditure information shall include the identification of the employee name, labor category, hourly labor rate, and total number of labor hours expended.
- Supplemental Accounting Code Information. The invoice shall include a supplemental electronic file that includes the name of each contractor employee, the number of hours worked in the month associated with the NITC accounting/shorthand code associated with the work performed. PWS Attachment E is provided for informational purposes.
- Supporting documentation for travel costs. Invoices including travel costs shall include supporting documentation as required by the Federal Travel Regulation (FTR) (receipts for all costs \$75.00 or greater). Invoice submissions including travel costs shall include completed travel expense sheets (i.e. travel voucher) for each trip for each employee.

8.6. Monthly Status Report

Monthly status reports shall include, but is not limited to, the items identified below.

- Status of task directives, schedules, deliverables. Status of task directives shall include a summary description and schedule of all task directives completed during the reporting period, all task directives currently on-going during the reporting period and all known task directives assigned for future reporting periods.
- current and cumulative task funding status (direct labor and travel funding status to be reported separately as required),
- outstanding issues, and proposed resolution approaches and actions to resolve any outstanding issues.
- Staffing report identifying current staffing roster, all current vacancies, and a record of all staffing departures
- Summary of the Scheduled Absence Calendar Availability deliverable for the two month period following the end of the MSR reporting period that clearly identifies and lists the scheduled absences
- Listing of all training to be completed within the two month period following the end of the MSR reporting period
- The monthly invoice shall be submitted simultaneously with the monthly status report.

8.7. Phase-In / Phase Out

8.7.1. Phase-In Plan

The contractor may or may not propose a separately priced transition period, for a duration to be determined and proposed by the contractor, but shall not exceed a period of 30 calendar days. The transition period is defined as the period of time (during the Phase-In) when the new contractor and the incumbent contractor will both be providing support to the client as required to support the transition to the newly awarded task order. If the contractor chooses to propose a transition period, such period shall be included and addressed within the below identified Phase-In Plan.

The Contractor shall develop a Phase-In Plan. Such Phase-In Plan shall present a clear understanding of the Phase-In tasks required, the issues likely to result from non-incumbent Contractor performance, and the Contractor's proposal to resolve such issues. The Phase-In Plan shall include a clear and feasible strategy for delivering services required within the periods specified by the Plan and shall include a detailed plan-of-action and milestones to transition the functions identified in this PWS in a well-planned, orderly, and efficient manner. The Phase-In Plan shall include, at a minimum:

- Staffing plan.
- Development and submission of required deliverables.
- Interface with the Government and incumbent contractor (if applicable) during Phase-In, to include meetings or status reports, as required.
- Approach to maintaining quality and minimizing disruption during Phase-In.
- Development and dissemination of operating instructions, procedures, and control directives.

8.7.2. Phase Out Plan

During phase-out of this task order, which is determined to be a period of 90 days prior to the lifecycle end date of the task order, a smooth and orderly transition between the incumbent contractor and the successor contractor is necessary to ensure a minimum disruption to vital Government business. The Contractor shall cooperate to the extent required to permit an orderly changeover to the successor Contractor. The phase-out will be deemed completed by the COR when it is determined by the Government that the transition of property, data, and information developed as a part of this task order have been successfully changed over from the outgoing Contractor to the Government and the successor Contractor as required. Phase out activities include, but are not limited to, the tasks below.

- Submission of official comprehensive phase out plan.
- Daily communication of staffing status (i.e. projection of when incumbent contractor employees will off-board from the incumbent task order and identification of additional incumbent resources, such as a transition team, that may be needed to support the transition efforts) and overall phase out status, in accordance with the accepted phase out plan.
- Maintain the phase out schedule included within the phase out plan.
- Transition of property.
- Transition of supporting documentation.
- Transition of accounts (e.g. user accounts and user access).
- Knowledge transfer on the established installation, operation, and maintenance procedures of the technologies supported. The phase out plan shall clearly describe the proposed methodologies to be utilized for such transfer (e.g., written documentation, manuals, formal classroom type training, one-on-one training sessions, etc.).
- Execution and submission of phase out checklist, to include Government acceptance.

8.8. Deliverable Matrix

Title	Description	Due Date
Quality Control Plan.	Refer to PWS paragraph 7.1.	Submission due concurrent with contractor quote. If requested, a final QCP shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 30 calendar days after task order award.
Monthly Invoice.	Refer to PWS paragraph 8.5.	The 15th calendar day of the month following the reporting period.
Monthly Status Report.	Refer to PWS paragraph 8.6.	The 15th calendar day of the month following the reporting period.
Phase-In Plan (Transition Plan).	Refer to PWS paragraph 8.7.1.	Submission due concurrent with contractor quote. If requested, a final plan shall be furnished for acceptance by the GSA Contracting Officer addressing any Government comments provided no later than 15 calendar days after task order award.
Phase Out Plan.	Refer to PWS paragraph 8.7.2.	120 calendar days prior to the period of performance end date.
Project Specific Deliverables.	Plans, Reviews, Assessments, Reports, etc.	To be determined at the time the project specific task directive is assigned to the

		contractor.
--	--	-------------

8.9. Other Reporting Requirements

In addition to the deliverable requirements identified above, the contractor shall comply with the following:

- The contractor shall bring problems or potential problems affecting performance to the attention of the COR as soon as possible. Verbal reports shall be followed up with written reports, when directed by the COR, within 24 hours.
- The contractor shall provide, in writing to the COR, the results of all meetings with the client that affect and/or change conditions or result in additional agreements or requirements. The contractor shall not perform any work outside the scope or requirements of this PWS and resultant order without express written approval of the CO.

9. PERFORMANCE

9.1. General

Work is to be accomplished through the General Services Administration (GSA), Federal Acquisition Service (FAS), Great Lakes Region, through its task order with the contractor. Certification by the Government of satisfactory services provided is contingent upon the contractor performing in accordance with the terms and conditions of the referenced task order, this document, the approved technical and cost quotes, and all amendments. The client's representative, GSA's representatives, and the contractor's representative(s) shall meet when deemed necessary at the client's request. The client representative, the GSA representatives, and the contractor's representative may meet at the place determined by the client representative and GSA representatives.

9.2. Kickoff Meeting

Within 7 days of contract award, the Contractor shall initiate work on this task order by meeting with key client agency representatives, to include GSA, to ensure a common understanding of the requirements, expectations, and ultimate end products. The contractor shall discuss the overall understanding of the project and review the background information and materials provided by the client. Discussions will also include the scope of work, deliverables to be produced, how the efforts will be organized and project conducted; assumptions made/expected and results. A concerted effort shall be made to gain a thorough understanding of the client agency expectations. However, nothing discussed in this or in any subsequent meetings or discussions between the client and the Contractor shall be construed as adding, deleting, or modifying any task order requirements, including deliverable specifications and due dates.

9.3. Period of Performance

The anticipated period of performances are identified below. The actual periods may be adjusted based on the duration of the transition period, if applicable.

Transition Period:	June 1, 2015 through June 30, 2015 (maximum duration)
Base Year:	July 1, 2015 through June 30, 2016
Option Year 1:	July 1, 2016 through June 30, 2017
Option Year 2:	July 1, 2017 through June 30, 2018
Option Year 3:	July 1, 2018 through June 30, 2019
Option Year 4:	July 1, 2019 through May 31, 2020

9.4. Place of Performance.

The Primary Place of Performance shall be in NITC government facilities. When required by the Government, the Contractor shall also perform Task Order related activities at other Government and Contractor facilities within the local area. For the purposes of this Task Order, local area facilities are defined as those within 50 miles of a Primary Place of Performance. Reimbursement for local area travel shall not be authorized. Contractor requests for alternate performance locations (i.e. telework and work from other Government

facilities) will be reviewed and considered on a case-by-case basis. The contractor shall obtain the required authorization prior to performing work at an alternate performance location. A list of the authorized NITC work locations are listed below. The work locations are subject to change.

- a) Kansas City, Missouri (NITC-KC) Main Location:
USDA National Information Technology Center
8930 Ward Parkway
Kansas City, Missouri 64114-3363
- b) St. Louis, Missouri Location at the Goodfellow Federal Complex:
United States Department of Agriculture
National Information Technology Center - STL
Goodfellow Federal Complex
4300 Goodfellow Blvd, Bldg. 104
St. Louis, Missouri. 63120
- c) Washington, D.C. (NITC-DC) Location:
USDA National Information Technology Center
Room S-100, South Building
1400 Independence Avenue, S.W.
Washington D.C. 20250
- d) Ft. Collins, Colorado Location:
USDA
Building A
2150 Centre Avenue
Fort Collins, Colorado 80526
- e) George Washington Carver Center (GWCC), Maryland Location:
USDA National Information Technology Center
George Washington Carver Center
5601 Sunnyside Ave.
Beltsville, Maryland 20705-5000
- f) Salt Lake City, Utah Location:
USDA-FSA-APFO
2222 West 2300 South
Salt Lake City, Utah 84119-2020
- g) Ft. Worth, Texas Location:
Fort Worth Federal Center
501 West Felix Street, Building 23
Fort Worth, Texas 76115

9.4.1. Applicability of Telework.

All work performed at locations other than those identified as Government and/or contractor facilities shall be approved prior to performing the work. Federal contractors are not governed by Office of Personnel Management (OPM), GSA, or the individual agency policies; however, this does not prohibit contract employees from actually working at an alternate site, when/as appropriate **and specifically authorized by the Government.** Contractor shall develop telework policies to comply with the following requirements and address at a generic level within their Quality Control Plan. Alternate work arrangements for contractors shall be negotiated with the contractor's own employer and the appropriate agency official, to ensure policies and procedures are in close alignment and there is a clear and concise arrangement documenting the agreement. It remains the contractor's responsibility to ensure the services are performed

in accordance with the terms and conditions of the award. The following are applicable telework classifications included within PWS Attachment C:

- No – No telework available.
- Situational – Occasional, pre-arranged telework.
- Limited – Specified number of days per week for telework.

9.4.1.1. Quality Control

The contractor shall address the pertinent facts impacting performance and ensure all affected contractor resumes reflect the applicable work site. The contractor shall provide justification to the Government when identifying and submitting an individual as a telecommuter and address implementation processes and procedures within the quality control plan. The contractor shall be responsible for ensuring the Government has the required access/details necessary for the Government to perform quality assurance responsibilities.

9.4.1.2. Compliance

The contractor shall comply with all agency security telework policies. The contractor shall ensure all services provided from an alternate site comply with the Federal Information Security Management Act of 2002 (FISMA) and address the following, as a minimum:

- Controlling access to agency information and information systems;
- Protecting agency information (including personally identifiable information) and information systems;
- Limiting the introduction of vulnerabilities;
- Protecting information systems not under the control of the agency that are used for teleworking;
- Safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- Preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

9.4.2. Travel

The Contractor shall also perform non-local travel in support of this Task Order, as required by the Government. The COR, or the appointed representative, shall have sole authority to approve non-local travel requests necessary to support Task Order performance. Not later than 5 business days prior to the Contractor's estimated date of departure, the Contractor shall submit to the COR, via ITSS, a travel request, to include travel justification, the proposed itinerary, and cost estimates for such travel. Federal Travel Regulations apply. The Contractor shall be responsible for all travel arrangements including airline, hotel, and rental car reservations. The Contractor shall make every commercially reasonable effort to schedule travel far enough in advance to take advantage of reduced airfares.

9.5. Hours of Work

The NITC is a shared services hosting provider (i.e., data center) that operates 24x7x365. Hours of support can and will be dependent on data center customer requirements for assigned tasks. The contractor shall coordinate work schedules with the COR to ensure service requirements are met, Government personnel are available, and customer results are achieved. The Contractor shall not exceed the monthly allocation of hours, calculated at 8 hours per day times the number of business days/month, without authorization from the COR. Additional details are provided below and the applicable work hour category for each CLIN is identified in PWS Attachment C.

9.5.1. Standard Duty Hours Support

The contractor shall provide for normal (during core business hours) and staggered standard duty hours support as required to ensure adequate coverage for US time zones.

9.5.1.1. Normal Workday - (work hour category A)

A standard normal workday is defined as any 8 hours of productive labor which must include the Core Business hours of 9:00 AM through 3:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, to include short-term or long-term requirements for staggered workdays.

9.5.1.2. Staggered Workday - (work hour category B)

A standard staggered workday requires that on-site support shall be provided 6:00 AM through 6:00 PM local time, Monday through Friday, excluding Federal Holidays. Exceptions may be required and shall be coordinated with the COR, if coverage is required outside the 6:00 AM – 6:00 PM timeframe.

9.5.2. Non-Standard Duty Hours Support

The contractor shall provide for scheduled (planned work hours) and un-scheduled (other than planned work hours), non-standard duty hours support as required. The contractor shall identify a primary and alternate point of contact for non-standard, un-scheduled duty hours requirements. To ensure the applicable labor hours allocations are not exceeded (typically 40 hours per week), labor hours expended in support of non-standard duty hours requirements shall be off-set by reducing the number of standard duty work hours by an equivalent number.

9.5.2.1. Scheduled (work hour category C)

Scheduled non-standard duty hours support shall be coordinated with the authorized Government point of contact and the contractor's designated point of contact. Customers may request non-standard duty hours support for their environments (usually quarterly and during peak release or operational periods). Scheduled non-standard duty hours support may also be required to support a short term surge in requirements.

9.5.2.2. Un-Scheduled (work hour category D)

The Government may also request that the contractor provide un-scheduled (e.g., emergency technical support), non-standard duty hours support. The contractor shall respond within 15 minutes of notification. When off-site support can resolve the issue, the contractor's personnel shall begin immediately upon notification. The contractor shall assess the cause, determine the scope of the problem, advise the appropriate Government organization, provide an estimated restoration time, and identify and implement action for problem resolution. When required, on-site support shall begin within one hour of notification to the contractor's designated individual. This unscheduled support may include:

- Remote telephone support with the Government Technical Staff and/or customers.
- Remote support on GFE. Contractor employees may be equipped with GFE that enables remote data center access/log-on. The Government will not incur any costs associated with home-based WiFi or LAN access to the Internet.
- Onsite support.

9.5.3. Continuity of Operations (COOP)/Disaster Recovery (DR)

The National Security Presidential Directive/NSPD-51/Homeland Security Presidential Directive/HSPD-20, National Continuity Policy, requires Federal departments and agencies to maintain a comprehensive and effective continuity capability, including a Continuity of Operations (COOP) program. The COOP program, which also includes pandemic preparedness, ensures the continuation of essential functions under emergency situations.

An emergency may require personnel to temporarily relocate to a pre-designated, alternate work site or telework to ensure continuity of essential functions. A contract position may support the NITC's COOP plan, and the contractor may be required to report for work to assist the NITC federal staff in supporting

critical business functions following a formal disaster declaration. Contract employees, under this scenario, are required to deploy to the alternate work site within 12 hours of COOP Plan activation for the support of government identified essential functions. The deployment to the alternative work site may last for up to 30 days. Travel and per diem expenses, if required, will be reimbursed in accordance with the Federal Travel Regulation (FTR).

NITC will also engage in "PLANNED" Disaster Recovery Exercises throughout a given Fiscal Year. As these exercises are typically planned well in advance, NITC may require contract employees' participation in these exercises after appropriately coordinated advance notice. There may also be the limited possibility of an "UN-PLANNED" Disaster Recovery Exercise. Unplanned exercises are typically conducted during business hours and NITC may require contract employees' participation after immediate notice. Travel is not expected to be required during DR Exercises/testing.

9.5.4. Holidays

The contractor is hereby advised that government personnel observe the following holidays: New Year's Day, Martin Luther King's Birthday, President's Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran's Day, Thanksgiving Day, and Christmas. In addition to the days designated as holidays, the government may observe the following days: any other days designated by Federal Statute; any other days designated by Executive Order; and any other days designated by the President's Proclamation. This includes Inauguration Day (Washington, D.C. metropolitan area only). Observance of such days by government personnel shall not be a reason for an additional period of performance, or entitlement of compensation. In the event the contractor's personnel work during the holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost.

9.5.5. Government Administrative Leave Situations

When the agency grants administrative leave to its employees, on-site assigned contractor personnel may be dismissed by the contractor. The contractor agrees to continue to provide sufficient personnel to perform task orders already in operation or scheduled, and shall be guided by the instructions issued by the COR. The Government will not pay for the labor hours during the leave granted to contract personnel as a result of inclement weather, potentially hazardous conditions, explosions, and other special circumstances.

10. GOVERNMENT FURNISHED EQUIPMENT/INFORMATION/ACCESS

10.1. General

The Government shall provide, without cost, the facilities, equipment, materials and services listed below. The Government furnished property and services provided as part of this task order shall be used only by the contractor only to perform under the terms of this task order. No expectation of personal privacy or ownership using any USDA electronic information or communication equipment shall be expected. All property at Government work sites, except for contractor personal items will be assumed to be government property unless an inventory of contractor property is submitted and approved by the CO/COR. Contractor personal items do not include computers, external drives, software, printers, and/or other office equipment (e.g., chairs, desks, file cabinets). The contractor shall maintain an accurate inventory of Government furnished property.

10.2. Property

10.2.1. Facilities

The Government will provide facilities at the authorized work locations specified in the task order. Use of the facilities by contractor employees will include all utilities, telephone, janitorial services and furniture for contractor employees performing tasks. The Government will provide the contractor access to buildings as required, subject to the contractor's employees obtaining the required security clearances.

10.2.2. Equipment at Authorized On-Site Federal Work Locations

The Government will provide the following at authorized on-site Federal work locations:

- a) A suitable work environment (i.e., telephone, office space and furniture).
- b) A personal computer/laptop and auxiliary hardware and software required in the performance of the task order.
- c) Network connectivity required to perform work assignments. Network and computer access rights commensurate with work assignments.
- d) Pagers, headsets, cell phones and maintenance agreements for such equipment when determined to be applicable by the COR. The Government will replace items that are determined to be beyond economical repair by the COR unless damage or loss is determined to be due to contractor negligence.

10.2.3. Facilities and Equipment at Remote Work Locations

When work from a remote location is authorized by the COR, the contractor will not be reimbursed for costs associated with remote connectivity from cell phones, WiFi access or Internet connection.

The contractor shall be responsible for ensuring the contractor employee has an adequate and safe office space that sufficiently protects Government equipment and information from loss, theft or unauthorized access. The contractor shall establish a telework agreement with the contract employee. The agreement, given a minimum of 24 hours of advanced notice, shall allow periodic inspections of the alternate work location can be undertaken. The purpose of the inspection is to ensure proper maintenance of Government-owned property and worksite conformance with safety standards and other specifications. The contractor is informed that telework is not a substitute for dependent care (i.e., child care or elder care) and that the appropriate arrangements must be made to accommodate children and adults who cannot care for themselves, while performing official duties of this contract at an alternate work location.

10.2.4. Materials

The Government shall furnish basic reference manuals, and any revisions, updates, and changes thereto for use by the contractor necessary to perform work assignments under the task order.

10.2.5. Validation of Government Furnished Items (GFI) and Equipment Inventory

The contractor shall develop and maintain a complete GFI inventory that shall be made available to the Government upon request. Within three (3) work days of receipt of any GFI, the contractor shall validate the accuracy of the materials and notify the COR, in writing, of any discrepancies.

NOTE: Validation shall consist of the Contractor checking for physical and logical completeness and accuracy. Physical completeness and accuracy shall be determined when all materials defined as Government furnished are provided, as defined in the task order. Logical completeness and accuracy shall be determined when all materials defined and associated with a program, system, or work package are provided.

10.3. Use of Government Property

10.3.1. Desk Telephones

Government telephones are provided for use in conducting official business. Contractor employees are permitted to make calls that are considered necessary and in the interest of the Government. The contractor will follow the same USDA and NITC policies as Government personnel the govern telephone usage.

10.3.2. Mobile/Wireless Telephones and Smart Devices

Government issued mobile/wireless telephone and smart devices may be assigned to contractor employees when the Government determines it is in the Government's best interest. Contractor employees are prohibited from using any Government issued device for personal use and would be subject to paragraph 10.3.9.

10.3.3. Mail/Postage

Contractor employees shall not have their personal mail directed to Government offices or use Government-furnished postage for personal benefit. The contractor shall follow the same USDA and NITC policies as Government personnel that govern mail usage including overnight delivery.

10.3.4. Electronic Mail (E-mail)

All Government e-mail access and use by contractor employees shall be in support of the individual's official duties and task responsibilities. All information that is created, transmitted, received, obtained, or accessed in any way or captured electronically using USDA's e-mail systems is the property of the Government. Contractor employees shall have clear identification in their e-mail signature block that identifies themselves as contractor employees in support of USDA NITC. Contractor employees are prohibited from forwarding e-mail generated from a Government provided e-mail account to personal mobile devices.

10.3.5. Copiers

Copiers are to be used to copy material for official Government business only in the performance of the tasks in this task order.

10.3.6. Fax Machines

Contractor employees shall not use fax machines for other than official Government business in the performance of the tasks in this task order.

10.3.7. Computer and Internet

All Internet and electronic media access accomplished by contractor employees (utilizing Government furnished equipment) shall be for official Government business in the performance of the tasks in this task order.

10.3.8. Canvassing, Soliciting, or Selling

Contractor employees shall not engage in private activities for personal gain or any other unauthorized purpose while on Government-owned or leased property, nor may Government time or equipment be utilized for these purposes.

10.3.9. Security Violations Using Government Equipment

Any contractor violating USDA security policies, guidelines, procedures, or requirements while using Government equipment or while accessing the USDA network may, without notice, have their computer and network access terminated, be escorted from their work location, and have their physical access to their work location removed at the discretion of the CO/COR. The CO/COR will notify the contractor of the security violation and request immediate removal of the contract employee.

10.4. Government Vehicles

The use of Government-furnished vehicles is NOT authorized under this task order. If a vehicle is needed to perform required services, it must be supplied by the contractor for their employees' official government business needs. This paragraph is not applicable to rental vehicles utilized during approved travel under the contract.

10.5. Return of Government Property

All Government property, data, software, information, documentation and equipment whether furnished by the Government to the contractor, created by the contractor, or acquired by the contractor with Government funding is property of the Government and shall be delivered/transmitted to the COR upon termination or expiration of the task order or per instructions from the CO.

10.6. Conservation of Utilities

The contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating practices that preclude the waste of utilities, which shall include:

- a) Lights shall be used only in areas where and when work is actually being performed.
- b) Mechanical equipment controls for heating, ventilation, and air conditioning system shall not be adjusted by the contractor or by contractor employees.
- c) Water faucets or valves shall be turned off after the required usage has been accomplished.

11. SECURITY

USDA/OCIO has established legal and regulatory requirements that must be met before access is granted to federal IT resources. In order to gain access to USDA computer networks and computers, contractor personnel are required to initially complete the following requirements including, but not necessarily limited to:

- The USDA Information Security Awareness and Rules of Behavior training (web or paper-based). Additional and/or different courses may be required as USDA and NITC security policies change.
- The instructions to obtain USDA E-Gov access (eAuthentication).
- The documentation required for a security background investigation, which includes the Federal Bureau of Investigation's (FBI) National Criminal History Check ("fingerprint check") and eQIP.
- Information needed to obtain a Personal Identity Verification (PIV) card.

The contractor shall be responsible for ensuring compliance by its employees with all applicable federal regulations, to include those of GSA, NIST, USDA and HSPD-12. Contractors and their employees are subject to all Federal laws applicable to Government installations and are under the jurisdiction of the Federal Protective Service (FPS). The NITC COR, in conjunction with the USDA-OCIO Personnel Security Specialist (PSS), will ensure that the contractor submits the required Security Background Investigations/Clearances.

In addition, the contractor shall be responsible for ensuring compliance by its employees for any annual security training and reporting requirements of GSA, NIST, USDA and HSPD-12. Any contract employee working under this OCIO/NITC task order will be expected to follow the process for obtaining access to systems and notifying the Government for the termination of access upon the completion of performance under this task order. The contractor shall inform the COR and other designated NITC personnel if any changes are made in the status of contractor employees that would impact his/her access to USDA computer systems, and to follow the correct protocol for the creation, expansion and/or termination of such access.

11.1. United States Citizenship

No less than 75% of the contractor personnel assigned to this task, specifically to provide direct CLIN support, shall be United States citizens.

11.2. Security Awareness Training

Contract personnel who have access to USDA networks and computers will be required to take all security training necessary as determined by the Government to maintain access to the USDA network and computers. Currently, this includes an annual two hour or less, web-based Information Security Awareness training module and specialized training depending on the job function. The security training exam must be passed prior to any computer-system accesses are granted. Prior to an employee start-date, a paper-based exam must be administered by the contract site manager. If the employee is not successful in scoring a passing grade (70% or higher) on the first or second attempt, the contractor will be requested to submit a new candidate for the vacant position.

As USDA security policy changes, additional and/or different courses may be required. Contractor roles and permissions will be reviewed by the Government with the same frequency and at the same level as Government employees. Access to Government facilities, networks, and computers will require contractors to follow all Government mandated security alerts, procedures, patches and upgrades.

11.3. Background Investigation Requirements

After proper submission of paperwork, the Government covers the costs of investigations and submits the investigation for processing of all required security investigations/clearances, unless identified differently within this section. The scope of the security/background check required and the forms to be completed shall be determined in accordance with the Common Identification Standard for U.S. Department of Agriculture Employees and Contractors, USDA Directive 4620-002. The Government sponsor for this process shall be the COR or Government representative appointed in writing by the CO. The contractor shall be responsible for the preparation and submittal of the required forms. The contractor personnel shall not be required or permitted to perform work prior to receipt of the required security approvals.

Prior to being engaged on this task order, the contractor's employee must first have been processed for a favorably adjudicated FBI fingerprint check. An unfavorable FBI fingerprint check will require that the contractor remove the employee from any further consideration pertaining to this task order.

The contractor should be aware of any of its employees possibly having had a background investigation through another government agency. The investigation, if verifiable by the Government and completed within the last 5 years, can be accepted by the Government in lieu of a FBI fingerprint check.

Fingerprinting Instructions: The COR will provide contact information to make arrangements for fingerprinting of the contractor employees. Fingerprinting instructions include:

- fingerprinting for Kansas City, MO based personnel can be accomplished by the Personnel Security Office (PSO) at 8930 Ward Parkway.
- fingerprinting for DC-based personnel can be accomplished by the PSO Assistant, at the USDA South Building or personnel at the Beltsville, Maryland data center; or,
- fingerprinting can be obtained from the local law enforcement agency after the PSO provides the fingerprint cards. The contractor shall pay for all costs of fingerprinting by local law enforcement agencies.

Background Investigations:

Assuming a prior favorable FBI fingerprint check has been verified, for taskings and task assignments that exceed 180 days in length, a full background investigation, processed through the Office of Personnel Management (OPM), will be required for all contract employees under this contract.

The background investigation, prior to being submitted to OPM, must be favorably reviewed at the local level by the PSO. The COR, working with the PSO, will determine what level of background investigation is required, based on the type and sensitivity of the duties and/or systems being accessed by the contractor. Current NITC policy requires processing of high-risk, public-trust investigations.

The Contractor is responsible for the immediate removal of employee(s) from the task order, if any person is identified as being a potential threat to the health, safety, security, general well-being, or operational mission of the USDA and its population. Additional items revealed in the background check that may be unacceptable are: conviction of a felony, a crime of violence or serious misdemeanor, a record of arrests for continuing offenses, adverse financial issues, or falsification of security documentation. As a reminder, an unfavorable FBI fingerprint check will eliminate a contractor's employee for further consideration under this task order. Additionally, if unfavorable information is noted on the security questionnaire or developed during the ongoing or final background investigation, the Government retains the right to have the employee immediately removed from the task order at the Government's discretion. Unless otherwise directed by the Contracting Officer, the contractor shall provide a replacement within ten (10) business days. New hires or substitute personnel are subject to the same security background requirements.

Special Procedures when the Data Center proper is the Primary Duty Station.

If a contractor's duty position at an NITC facility is located within the data center space, the additional provisions of NITC Directive A8 must be adhered to. Primarily, the contractor shall be required to have an

investigation at the BI level. In addition to the favorable FBI Fingerprint check, the contractor must complete the online security questionnaire portion of the BI level investigation, which must then be favorably reviewed at the local level by the PSO's office. The online security questionnaire process must be initiated by the PSO and involves the use of the eQIP (Electronic Questionnaire for Investigation's Processing) system. Data center access cannot be approved until the online security questionnaire portion of eQIP has been completed, and the NITC Director or designee has approved the access.

11.4. Access to Sensitive/Critical Data

Contractor access to data deemed sensitive and/or critical by the Government will follow guidelines set forth in FIPS Publication 199, USDA and NITC security policy and only following successful completion of all security training.

11.4.1. Non-Disclosure Agreement.

Due to the sensitive nature of the data and information being worked with on a daily basis, all Contractor personnel assigned to the Task Order are required to complete the Government provided non-disclosure agreement within 15 calendar days after Task Order award, or prior to task order assignment, to ensure information that is considered sensitive or proprietary is not compromised. Signed non-disclosure statements shall be provided to the COR.

11.4.2. Data Access

The contractor may be required to have access to live production data for the performance of this task order. Any records and data or information the contractor may have access to may be highly sensitive and confidential. The contractor shall not divulge or misuse any information about files, data processing activities or functions, user IDs or passwords, or any other knowledge that may be gained, to anyone who is not authorized to have access to such information. It is the contractor's responsibility to ensure that other persons have the proper authorization

11.5. Security Incident Reporting

Contractors shall report the loss or suspected loss of equipment or paper-based data including Sensitive but Unclassified (SBU) or Personally Identifiable Information (PII) information according to the NITC Incident Response Policy when the contractor or contractor's employee first becomes aware of the loss or suspected loss. If the contractor or contractor's employee does not have access to this procedure, then the incident should be immediately reported to the Agriculture Security Operations Center (ASOC) via the 24-hour Cyber Incidents Hotline, (866) 905-6890.

11.6. Permanent Security Badge Requirements

A permanent security badge will not be issued until the security questionnaire has been completed and favorably reviewed. In order to gain access to NITC authorized work locations via a permanent security badge, all contractor employees are required to complete the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005). The contract employee will be given this form upon first arrival for duty by the Contractor. Form Number AD-1197 (Sept. 2005) requires two (2) forms of identification be submitted. Contract employees are required to provide this identification when first reporting for work. One form of identification must any one of items 1-4 in the list below (Primary ID). The other ID may be any of the forms of ID listed below (Primary or Secondary ID types).

Acceptable Forms of ID:

Primary Forms of Identification (Items 1-4)	
1. US Passport (unexpired or expired)	3. US Military ID card (unexpired)
2. Driver's license or ID card issues by a state or possession of the United States provided it contains a photograph (unexpired)	4. US Military Dependent's ID Card (unexpired)

Secondary Forms of Identification (Items 5-25)	
5. US Social Security Card issued by the Social Security Administration	16. Permanent Resident Card or Alien Registration Receipt card with photograph (Form I-151 or I-1551)
6. Original or certified copy of a birth certificate issued by a state, county, municipal authority, or outlying possession of the United States bearing an official seal	17. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350)
7. ID issued by federal, state, or local government agencies or entites, provided it contains a photograph.	18. Unexpired Temporary Resident Card (Form I-668)
8. School ID with photograph	19. Unexpired Employment Authorization Card (Form I-668A)
9. Voter's registration card	20. Unexpired Reentry Permit (Form I-327)
10. US Coast Guard Merchant Mariner card	21. Unexpired Refugee Travel Document (Form I-571)
11. Certificate of US Citizenship Form (Form N-560 or N-561)	22. Unexpired employment authorization document issued by DHS
12. Certificate of Naturalization (Form N-560 or N-570)	23. Unexpired Employment Authorization Document issued by DHS with photograph (Form I-668B)
13. US Citizen ID Card (Form I-197)	24. Driver's license issued by a Canadian Government Authority
14. Unexpired foreign passport with I-551 stamp or attached Form I-94 indicating unexpired employment authorization	25. Native American tribal document
15. ID card for use of Resident Citizen in the United States (Form I-179)	

11.7. Display of Permanent Security Badges

A permanent security badge must be worn at all times while in the facility. It must be displayed above the waist. The individual will retain possession of the permanent security badge as long as continued admittance to the site is needed. Ensuring the safekeeping, wearing, and visibility of Government furnished security badge is the responsibility of the person issued a USDA Identification (ID) Badge. A permanent security badge shall immediately be returned to the Government when the need for it ceases to exist.

11.8. Temporary Security Badge Requirements

The Contractor shall ensure that each of the contractor's employees has been issued a temporary badge while the Request for USDA Identification (ID) Badge, Form Number AD-1197 (Sept 2005) is being proceeded. Temporary or visitor badges will be provided for persons who are identified as having an infrequent or temporary legitimate business need for access to the site. As noted above, tasks and task assignments that exceed 180 days will require a permanent badge. The temporary badge authorizes the wearer to enter and exit the secured areas where NITC workstations are located within applicable authorized work location. The badge

must be worn at all times while in the facility. It must be displayed above the waist. The badge must be returned to the security desk at the close of the business day.

11.9. Facility Security Requirements

Due to NITC facility security policies, it is required that the facility guards be notified in advance of all visitors wanting to enter the facility. This 24-hour advanced notification must provide the names, dates, times, the nature of the visit and the visitor's point of contact (POC). All visitors must have a NITC POC in order to be admitted to the facility. Individuals arriving at the NITC data center facilities that do not provide a pre-arranged POC may be turned away.

- 8930 Ward Parkway Facility Visitors Entrance. The east lobby of the 8930 Ward Parkway facility is the entry point for all NITC visitors. Visitors shall check-in at the east lobby guard station, sign-in and be issued a visitor's badge. The visitor's POC will be notified of the visitor's arrival. The visitor will be screened by a hand-held magnetometer, and the visitor's belongings will be passed through an x-ray machine. Failure to voluntarily comply with these security measures will cause the visitor to be denied access to the facility. The visitor shall return all issued visitor's badges at the end of the day or upon leaving the facility for any reason. Point of Contact: PWS COR.
- St. Louis, Missouri Location at the Goodfellow Federal Center Complex. Entrance onto the Federal Center Complex is at the main gate accessible from Goodfellow Boulevard. The main gate is open 24/7 and manned by GSA security officers. All vehicles entering the Campus are required to have a permanent complex decal or a Federal Center Complex parking permit. This must be arranged with the point of contact before attempting to enter the Federal Center Complex. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. Visitors must sign in at the main entry and be on the entrance list prior to attempting to enter the Federal Center Complex. The visitor is issued a paper badge which is returned upon leaving the Complex. The visitor's point of contact (POC) is notified to come to the gate and escort the individual. The POC will coordinate the access requirements with the lead Agency, Rural Development. Point of Contact: Diego Maldonado, Diego.Maldonado@ocio.usda.gov.
- Washington, D.C. (NITC-DC) Location. The COR must sponsor all contract employees into the Whitten-South Building Complex. To process a contractor for a site identification badge, the federal sponsor must submit a form to, Tawana Waller, the headquarters security contact for all Office of the Chief Information Officer organizations. Once the proper background checks and security process determined to be adjudicated acceptably, the contractor would report to Room 1408-South (1st floor, 4th wing) for photo identification badging. Point of Contact: Bryan Dixon, Bryan.Dixon@ocio.usda.gov.
- George Washington Carver Center (GWCC), Beltsville, Maryland Location. The main entrance to the Carver Center is at Building 1. Building 1 has a 24x7 guard posted at the reception desk. Visitors check-in check at Building 1 reception desk, show a valid identification, sign-in and issued a visitor's badge and parking permit. The visitor's belongings are then passed through an x-ray machine. The visitor's POC will be notified of their arrival and escorted within the facility. Badging office is located in Building 1 just east of the reception desk. Point of Contact: Bryan Dixon, Bryan.Dixon@ocio.usda.gov.
- Salt Lake City, Utah Location. The facility is open from 6am-6pm/Mountain time, Monday-Friday (closed Federal holidays). The facility is open to the general public. The public entry point is at the East side of the facility next to the flagpole. All general public are required to sign in, issued a temporary day-use visitor pass. Visitors needing access beyond the Customer Service Area need to be escorted by the POC. The visitor's POC will be notified of their arrival and escorted within the facility. Point of Contact: Lori Uhlhorn, lori.uhlhorn@slc.usda.gov; Denny Skiles, denny.skiles@slc.usda.gov.
- Ft. Worth, Texas Location at the National Geospatial Center of Excellence with the Fort Worth Federal Center. The Fort Worth Federal Center entrance is at the main gate at 501 W. Felix Street. Boulevard. The main gate is open 24/7 and manned by GSA security officers. Visitors are required to undergo a vehicle inspection conducted by the guards at the gate. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the gate and escort the

individual. The POC will coordinate the access requirements to Building 23 or 24, as applicable. Point of Contact: Paul Fukuhara, paul.fukuhara@ftw.usda.gov

- Ft. Collins, Colorado location at the Forest Services' Natural Resources Research Center, Building A, on the Colorado State University campus. The Natural Resources Research Center (NRRC) is located at 2150 Centre Avenue, Building A, Fort Collins, CO 80526. The main entrance is during normal business hours to visitors. The visitor's point of contact (POC) should be notified 24 hours in advance. The visitor's POC will be notified to come to the entrance and escort the individual. The POC will coordinate the access requirements to the building, as applicable. Point of Contact: Rick Rohlf, rick.rohlf@ocio.usda.gov; Jordan Bancroft, (970-295-5710).

11.10. Parking Requirements

The contractor shall direct its employees to comply with applicable rules governing parking at each authorized work location. These rules may include the display of a parking permit in the windshield of a vehicle or the application of a parking permit to the exterior of a vehicle.

- 8930 Ward Parkway Facility Parking Requirements: The Contractor shall ensure that each contractor employee obtains a parking permit tag from the Government Security Staff. The tag shall be properly displayed and visible on any vehicle parked near the 8930 Ward Parkway physical plant. Vehicles only intermittently visiting the 8930 Ward Parkway facility shall park in the visitor parking area.
- St. Louis, Missouri Location at the Goodfellow Federal Complex: All vehicles on the Federal Center Complex grounds must have a permanent window decal or a Federal Center parking permit. Contact the St. Louis facility POC for arranging the appropriate vehicle pass.
- Washington, D.C. (NITC-DC) Location: There is no government provided parking available at this location.
- George Washington Carver Center (GWCC), Beltsville, Maryland Location: There is a separate parking area designated for visitors. USDA and contract employees from other locations are required to check in at the reception desk and get a temporary parking permit and park in employee parking area. Contact the GWCC POC for arranging the appropriate vehicle pass.
- Salt Lake City, Utah Location: The main parking lot is located East of the building with smaller lots located North and South of the main building. Contact the Salt Lake City for arranging the appropriate vehicle pass.
- Ft. Worth, Texas Location: From the guardhouse, proceed downhill, across the railroad tracks and take the second right. As you turn right you will go under Hemphill Street. Follow the street as it curves to the left. Yield at the sign, then cross the street into the parking lot on the east side of Building 23. Visitor parking is designated. Enter the building through the automatic doors under the blue awning. Contact the Fort Worth POC to arrange for a permanent vehicle pass.
- Ft. Collins, Colorado location: There are separate designated parking spaces for visitors. A temporary parking permit must be displayed on the dashboard of visitor vehicles. The temporary parking permit will be provided by the guard in Building A. Contact the Ft. Collins POC to arrange for a permanent vehicle pass.

12. ADMINISTRATIVE CONSIDERATIONS

12.1. Government Representatives

GSA Contracting Officer's Representative
Wendi Borrenpohl
1710 Corporate Crossing, Ste. 3
O'Fallon, IL 62269
618.622.5806
wendi.borrenpohl@gsa.gov

GSA Contracting Officer
Yjuania Still
1710 Corporate Crossing, Ste. 3

O'Fallon, IL 62269
618.622.5809
yjuania.still@gsa.gov

Client Contracting Officer's Representative
Carrie Coffman
USDA, NITC, Resource Management Division (RMD)-RSSB
8930 Ward Parkway
Kansas City, MO 64114
816.823.1249
carrie.coffman@ocio.usda.gov

12.2. Procedures for Payment

12.2.1. Performance Based Payment Percentages

The performance objectives and respective payment percentages based on relative importance to total task performance are identified in the CLIN descriptions contained in PWS Attachment A. This document also identifies the Government's proposed surveillance assurance methodology.

12.2.2. Submission

Invoices are due no later than the 15th calendar day of the month following the reporting period. The contractor shall submit the invoices and supporting documents, through ITSS simultaneously with the MSR (as an acceptance item) to allow the client and the COR to electronically accept and certify services received by the client representative. The contractor is authorized to invoice only for the services and travel ordered by GSA and provided in direct support of the task order.

12.2.3. Non-Compliance

Failure to comply with the procedures outlined may result in payment being delayed at no additional cost to the Government.

12.3. Personal Service

The client determined that use of the GSA requirements contract to satisfy this requirement is in the best interest of the Government, economic and other factors considered, and this task order is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 titled "Personal Services Contract". The Contractor agrees that this is a non-personal services task order. The Contractor is not, nor shall it hold itself out, to be an agent or partner of, or joint venture with, the Government. The Contractor agrees that his/her personnel shall neither supervise nor accept supervision from Government employees.

12.4. Section 508

All services and products provided in response to the requirements identified in this document shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d), and the Architectural and Transportation Barriers Compliance Board Electronic and IT (EIT) Accessibility Standards (36 CFR part 1194).

12.5. Privacy Act

Work under this task order requires that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and applicable USDA rules and regulations.

ID05140054 Performance Standards and Acceptable Quality Levels for all Labor Hour Contract Line Item Numbers (CLINs) (CLIN 013 through CLIN 029)		
Support Item / Area	Performance Standard	Acceptable Quality Level (AQL)
Availability	<ul style="list-style-type: none">■ 100% contractor personnel availability during required daily core hours or specific CLIN required schedules (with the exception of coordinated absences).■ The contractor is responsible for resource substitution/coverage when a coordinated absence is greater than five consecutive work days.	<p>No more than the identified violations as bulleted immediately below, per month.</p> <ul style="list-style-type: none">- CLINs with 1 to 5 individual task order performers providing support shall have no more than 4 violations.- CLINs with 6 to 10 individual task order performers providing support shall have no more than 6 violations.- CLINs with 11 to 15 individual task order performers providing support shall have no more than 8 violations.- CLINs with 16 to 20 individual task order performers providing support shall have no more than 10 violations.- CLINs with 21 to 30 individual task order performers providing support shall have no more than 12 violations.- CLINs with 30 to 40 individual task order performers providing support shall have no more than 14 violations.- The Government reserves the right to incorporate additional AQLs as needed consistent with those identified. <p>No more than 50% of the monthly violations shall be performed by an individual task order performer for CLINs that are supported by five or more individual task order performers.</p> <p>Each violation may be reflected as such within the CPARS assessment.</p>
Work/Task Product Activities	<ul style="list-style-type: none">■ All operational support activities shall be conducted in accordance with governmental & organizational standards, policies, directives, standard operating procedures, work instructions, processes & guidance. All operational support activities shall be captured and properly documented in the organizational ITSM tool. The contractor shall adhere to this requirement unless a written exemption is issued by an authorized Government representative.	<p>No more than the identified violations as bulleted immediately below, per month.</p> <ul style="list-style-type: none">- CLINs with 1 to 5 individual task order performers providing support shall have no more than 4 violations.- CLINs with 6 to 10 individual task order performers providing support shall have no more than 6 violations.- CLINs with 11 to 15 individual task order performers providing support shall have no more than 8 violations.- CLINs with 16 to 20 individual task order performers providing support shall have no more than 10 violations.- CLINs with 21 to 30 individual task order performers providing support shall have no more than 12 violations.- CLINs with 30 to 40 individual task order performers providing support shall have no more than 14 violations.- The Government reserves the right to incorporate additional AQLs as needed consistent with those identified. <p>No more than 50% of the monthly violations shall be performed by an individual task order performer for CLINs that are supported by five or more individual task order performers.</p> <p>Each violation may be reflected as such within the CPARS assessment.</p>
Security Incident Notification and Resolution	<ul style="list-style-type: none">■ 100% of security incidents, Personally Identifiable Information (PII) incidents, and lost or stolen equipment shall be reported within one hour of detection to the NITC Cyber Security Incident Response Team (NITC CSIRT) or the NITC Service Desk (888-USE-NITC or 816-926-6660).■ 100% of violations of security agreement terms or deliberate actions to circumvent security controls shall be addressed in accordance with Government direction.	<p>No allowable violations per month for any CLIN.</p> <p>In the event of a security breach that requires credit and fraud monitoring to be provided to those impacted, the contractor shall be liable for all costs associated with such monitoring.</p> <p>Each violation may be reflected as such within the CPARS assessment.</p>

CLIN Number	CLIN Title	CLIN Type	Estimated Core FTE	Estimated Varying Skill Levels for Core FTE	Applicable Work Hours	Required Work Location	Telework Authorization	COOP/DR Participation	ITSM Requirements
001	Audit Support Services	FFP	3	n/a - FFP	A	KC	LIMITED	NO	NO
002	Budget Analysis Support Services	FFP	1	n/a - FFP	A	KC	NO	NO	NO
003	Business Continuity Planning Services	FFP	1	n/a - FFP	A	KC	LIMITED	YES	NO
004	Enterprise IT Services Portfolio Management	FFP	2	n/a - FFP	A	KC	LIMITED	NO	NO
005	Facilities Operations Services	FFP	1	n/a - FFP	A, C&D	KC	SITUATIONAL	YES	NO
006	Information Systems Security Support Services	FFP	2	n/a - FFP	A	KC	LIMITED	NO	NO
007	ITSM Process Development and Documentation Services	FFP	1	n/a - FFP	A	KC	LIMITED	NO	YES
008	ITSM Service Asset and Configuration Management Support Services	FFP	2	n/a - FFP	A	KC	LIMITED	NO	YES
009	Program/Project Management Review Support Services	FFP	3	n/a - FFP	A	KC	SITUATIONAL	NO	NO
010	Task Order Management	FFP	2	n/a - FFP	A	KC	SITUATIONAL	NO	NO
011	Technical Architecture Support Services	FFP	3	n/a - FFP	A	KC	LIMITED	NO	YES-some within CLIN
012	Technical Writer	FFP	0	n/a - FFP	A	KC	LIMITED	NO	NO
013	ADDM Administration & Modeling Services	LH	1	n/a	A, C&D	KC	LIMITED	YES	YES
014	Application Integration Engineering Support Services	LH	15	YES	A, C&D	14 KC and 1 DC	LIMITED	YES -some within CLIN	YES-some within CLIN
015	Data Center Hardware Support Services	LH	2	NO	A	KC	NO	YES	YES
016	Database Administration Services	LH	8	YES	A, C&D	7 KC and 1 DC-	LIMITED	YES	YES
017	Mainframe Systems Programming Services	LH	0	n/a	A	KC	LIMITED	YES	YES
018	Network Engineering Services	LH	4	YES	A, C&D	KC	LIMITED	YES	YES
019	Remedy Engineering and Administration Services	LH	1	n/a	A, C&D	KC	LIMITED	YES	YES
020	Security Administration Services - AD & Identity Management	LH	7	YES	B, C&D	6 KC and 1 FTC	LIMITED	YES	YES
021	Security Administration Services - MF Auth., Role Mgmt. & Access Cont.	LH	1	n/a	A, C&D	KC	LIMITED	YES	YES
022	Security Engineering - Assessment Services	LH	1	n/a	A, C&D	KC	LIMITED	NO	YES
023	Security Engineering - Monitoring, Detecting & Analysis Services	LH	2	YES	A, C&D	KC	LIMITED	YES	YES
024	Security Engineering - Network Access Control Services	LH	3	YES	B, C&D	3 KC	LIMITED	YES	YES
025	Senior Application Engineering Services	LH	0	n/a	A	WDC	LIMITED	NO	NO
026	Server Automation Tool Support Services	LH	1	n/a	A	KC	LIMITED	YES	YES
027	Storage Administration Services	LH	7	YES	A, C&D	3 KC; 1 STL; 1 FTW; 1 FTC; 1 SLC	LIMITED	YES	YES
028	Systems Administration Services	LH	19	YES	A	19 KC	LIMITED	YES	YES
029	Systems Monitoring Administration Services	LH	3	NO	A, C&D	KC	LIMITED	YES	YES



NITC Manual

Human Resources Management Contractor In-Processing



For Internal Data Center Personnel

SHORT REFERENCE

ACM-0015-01

(Revision 2)

UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114

UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114

NITC MANUAL	SERIES: ACM NUMBER: 0015 – 01 REVISION:
SUBJECT: NITC Directive Management Program NITC Contractor In Processing	EFFECTIVE DATE: August 26, 2011 LAST AMMENDMENT DATE: n/a
APPROVED BY: Deputy Associate Chief Information Officer -Business, Finance & Security	OPI: Resource Management Division /Contract Management Branch AUTHOR: Phil Gehrt

AMENDMENT HISTORY

AMENDMENT DATE:	SECTION NAME / PARAGRAPH:	SUMMARY:	APPROVED BY:

UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114

REVIEW AND REVISION HISTORY

RELEASE DATE:	
NEXT RELEASE:	

REVIEW DATE:	REVIEWER NAME:	ACTION TAKEN:

REVISION DATE:	REVISOR NAME:	SUMMARY OF CHANGES:
08/24/11	Sue Brackney	Applying NITC Standard Template to the contractor process.
10/12/11	Sally Soule	Reformat Section 6
01/29/2014	Carrie Coffman	-Changed PPSO to PSO (Personnel Security Office) -Changed WCTS to ITS -Changed COTR to ACORT

NATIONAL INFORMATION TECHNOLOGY CENTER MANUAL

TABLE OF CONTENTS

Table of Contents	Page
AMENDMENT HISTORY	2
REVIEW AND REVISION HISTORY	3
TABLE OF CONTENTS.....	4
1. PURPOSE	5
2. SOURCES OF AUTHORITY AND REFERENCES	5
3. SPECIAL INSTRUCTIONS/CANCELLATIONS	5
4. POLICY	5
5. RESPONSIBILITIES	6
6. PROCEDURES.....	6
APPENDIX A REPORTS AND FORMS.....	A-1
APPENDIX B ABBREVIATIONS	B-1
APPENDIX C BLANK.....	C-1
APPENDIX D CHECKLIST FOR NEW CONTRACT EMPLOYEES.....	D-1
APPENDIX E NON-DISCLOSURE AGREEMENT	E-1

NATIONAL INFORMATION TECHNOLOGY CENTER MANUAL

1. PURPOSE

This manual describes the NITC Contractor In-Processing process.

The purpose of this Contract Employee In-Processing Manual is to establish an overview of procedures for the in-processing of contractor employees of the National Information Technology Center (NITC).

2. SOURCES OF AUTHORITY AND REFERENCES

Authority for managing the Human Resources Management Contractor In Processing and function is authorized by law and regulations, as follows:

- a. DR 1550-002, Building Safety/Security Occupant Emergency Program
- b. DR 3140-001, USDA Information Systems Security Policy
- c. DM 3545-001, Computer Security and Training, Chapter 9 Pt. 1
- d. DM 4620-002, Common Identification Standard of U.S. Department of Agriculture Employees and contractors.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This manual creates the ACM-0015-01, "Contractor In-Processing Procedures", Basic, dated August 26, 2011.

4. POLICY

- a. This NITC Contractor In Processing must be followed with all required forms completed in order to comply with, and satisfy, the above-mentioned authorities and references.
- b. Scope: This manual applies to all new/in-coming contract employees to all NITC locations (Kansas City, Ft. Collins, St. Louis, D.C., and Maryland).

5. RESPONSIBILITIES

a. Resource Management Division / Contract Management Branch

- (1) Issues directives and revisions to existing directives
- (2) Notifies the RO when a directive is deemed obsolete

b. NITC Senior Staff (including Required Clearance Officials).

- (1) Reviews and/or comments on each draft directive
- (2) Indicates concurrence with the draft via electronic signature, electronic initials, or voting features

c. Signing Authority.

- (1) Signing authority for this process will be the DACIO for Business, Finance & Security

6. PROCEDURES

a. Contractor Site Manager

Site managers are responsible for completing and maintaining the NITC Checklist for New Contract Employees (Attachment 1). This checklist should be utilized throughout the on-boarding process, including check-in. An outline of the site manager's responsibilities includes:

- (1) Requests work space/cubicle establishment
- (2) Facilitates appropriate systems access and privileges
- (3) Ensures all required forms have been completed, filed and submitted
- (4) Ensures all staff functions such as time charging, training, daily operational
- (5) Familiarization, performance plans and status reporting have been completed and/or addressed
- (6) Proctor Security Awareness Training and Test
- (7) Ensures completion of Records Management Training and Testing

- (8) Provide A-CORT copy of completed Attachment 1 and all required forms

b. NITC COR (RMD-RSSB)

- (1) Competes Form AD-1197, Request for USDA Identification (ID) Badge.
- (2) Copy Contractor-provided two (2) forms of identification.
- (3) Provide form 1197 and copy of identification to SPB physical security.
- (4) Enters contract employee data into Contractor Reporting System (CRS)
- (5) Provides Non-Disclosure Agreement to Contractor to sign and maintains copies (Attachment 2)

c. NITC A-CORT

- (1) Verifies work space/cube establishment
- (2) Verifies that appropriate systems access and privileges are requested
- (3) Verifies all required forms have been completed, filed and submitted
- (4) Verifies all staff functions such as time charging, training, daily operational familiarization, performance plans and status reporting have been completed and/or addressed
- (5) Provides correct account code(s) to use on timesheets (enters into CRS)
- (6) Ensures that Security Awareness and Records Management Certifications have been successfully completed
- (7) Ensures that all parties in Section 6 (d) – 6 (m) are notified as appropriate to perform tasks
- (8) Maintain official records for contract employee, including a copy of completed Attachment 1

d. Facilities Manager

- (1) Coordinates and maintains work space/cubicle establishment

e. NITC Service Desk

- (1) Generates tickets/work orders to establish work space/cubicle and system access

f. Network Services Branch

- (1) Provisions and maintains telephone, directory and LAN access in the work space/cubicle
- g. ITS Service Desk
 - (1) Generates tickets/work orders to configure LAN, e-mail access and contract employee orientation
 - (2) Installs IT equipment (desktop, laptop, printer, etc)
- h. Personnel Security Office (PSO)
 - (1) Enter contract data into NEIS and WebSETS
- i. Service Portfolio Branch (SPB)
 - (1) Obtains identification, photo and biometrics of the employee
 - (2) Completes and files forms for, and issues identification for physical and system access and parking
 - (3) Provides employee with required new-hire packet, including, but not limited to: parking decal, USDA/OCIO policies, OCIO Security Agreement and Occupant Emergency Plan
- j. Contingency Planning
 - (1) Enters and maintains contract employee information into the emergency call tree system
- k. Local Registration Authority (Security Division)
 - (1) Verifies identification of contract employee for appropriate level of system access
 - (2) Establishes ACF2 mainframe ID, if required
 - (3) Establishes mainframe access
- l. Training Coordinator or Designee
 - (1) Grades Security Awareness Training test.
- m. Administrative Assistant
 - (1) Assists offices with form completion and tasks as listed above.

n. Contract Employee

The contract employee will assist in the completion of the NITC Contractor's Checklist for New Contract Employees managed by the site manager (Attachment 1) where necessary. An outline of the contract employee's responsibilities includes:

- (1) Completes and submits all required forms as a new contract employee, and on an ongoing basis
- (2) Provides identification documents as required
- (3) Completes all required training for establishment of access into accounts

END

APPENDIX A

REPORTS AND FORMS

TABLE A1

REPORTS

NUMBER	REPORT TITLE	DESCRIPTION	SOURCE
None for this amendment.			

TABLE A2

FORMS

NUMBER	TITLE	DISPLAY	REFERENCE
None for this amendment.			

APPENDIX B

ABBREVIATIONS

TABLE B1

Abbreviation	DEFINITION
ACORT	Alternate Contracting Officer's Representative – Technical
CMB	Contract Management Branch
ITS	International Technology Services
LAN	Local Area Network
NEIS	Non-Employee Information System
NITC	National Information Technology Center
PSO	Personnel Security Office
RMD	Resource Management Division
SPB	Service Portfolio Branch

APPENDIX C

(Page left blank for future revisions)

APPENDIX D

CHECKLIST FOR NEW CONTRACT EMPLOYEES



Office of the Chief Information Officer

NITC COTR Checklist for New Contract Employees

AREAS	ITEMS	RESOURCES
Pre-Arrival		
Workspace	<input type="checkbox"/> Cube Location Approval <input type="checkbox"/> OALAN Account Form <input type="checkbox"/> PC & Printer <input type="checkbox"/> Phone	PPSEO/Building and Facilities WCTS Helpdesk Network Services Branch
Arrival		
Facility & Introductions	<input type="checkbox"/> Building Tour <input type="checkbox"/> Parking & Entrances <input type="checkbox"/> COTR	Site Manager
Time Tracking	<input type="checkbox"/> Entering Project Codes on Contractor Spreadsheet	COTR
Security	<input type="checkbox"/> Security Awareness and Privacy Training <input type="checkbox"/> COOP & LDRPS Contact Information	COTR NITC Contingency Mgmt. Group
PPSEO	<input type="checkbox"/> ID Card & Fingerprint Access <input type="checkbox"/> ID Badge	PPSEO

RMD-CMB	<input type="checkbox"/> AD 1197 form	COR
Immediate: To be accomplished within first days of reporting and no later than 30 days.		
PPSEO	<input type="checkbox"/> Parking Pass <input type="checkbox"/> OPM Background Investigation <input type="checkbox"/> Remote Access Agreement & Account (if applicable)	PPSEO Representative
Workspace	<input type="checkbox"/> Computer/Logon, LAN Directory, & Outlook <input type="checkbox"/> Phone <input type="checkbox"/> Office Supplies <input type="checkbox"/> Blackberry /Lap Top (if applicable) <input type="checkbox"/> NITC Contractor Reporting System	WCTS Helpdesk Network Services Branch COTR
NITC Policies and Procedures	<input type="checkbox"/> Directives	W:CENTER\DIRECTIVE-ADMIN or SECURITY
Training	<input type="checkbox"/> EAuth Account <input type="checkbox"/> Security Awareness Training <input type="checkbox"/> Ag Learn Account <input type="checkbox"/> Security Agreements <input type="checkbox"/> GETS Card	www.aglearn.usda.gov COTR/Site Manager
Administrative Support	<input type="checkbox"/> Scheduling of Conference Rooms <input type="checkbox"/> Scheduling the Conference Line (Meet-Me-Line) or Conference Bridge Line	Division Administrative Assistant

Internet Sites & NITC Information	<ul style="list-style-type: none"> <input type="checkbox"/> OCIO Intranet <input type="checkbox"/> USDA Directives <input type="checkbox"/> Occupant Emergency Plan NITC (KC Facility Only) <input type="checkbox"/> Emergency Notification Personal Information <input type="checkbox"/> NITC Emergency Hotline 	www.ocio.usda.gov/nitc www.ocio.usda.gov www.ocio.usda.gov/directives N:\Vital Records\Occupant Emergency Plans Security Governance Branch 877-333-4554
Intermediate: Areas will be ongoing and dependent upon position.		
System Access	<ul style="list-style-type: none"> <input type="checkbox"/> Mainframe ID and Permissions <input type="checkbox"/> Secure Remote <input type="checkbox"/> MS Project <input type="checkbox"/> Citrix <input type="checkbox"/> Big Brother Drill Down Menus <input type="checkbox"/> LAN Access <input type="checkbox"/> Account Users <input type="checkbox"/> Connections Account 	COTR will determine if access is required

APPENDIX E



NON-DISCLOSURE AGREEMENT

**United States
Department of
Agriculture**

**Office of the
Assistant Secretary
for Administration**
Departmental
Management

August 8, 2011

TO:

Management Services

Procurement
Operations Division

FROM: Pamela A. Yancey
Director, Resource Management Division (RMD)

Reporters Building
300 7th Street, SW
Suite 353
Washington, DC
20024

SUBJECT: Non-Disclosure Agreement

The Office of Federal Procurement Policy Act of 1988, as revised by the Clinger-Cohen Act of 1996, has established restrictions related to FAR 3.104, Procurement integrity. Congress has addressed the ethics and integrity of both Federal and private personnel in setting forth prohibitions against certain practices. These restrictions apply to any person who is a present or former official of the United States, is acting or has acted on behalf of, or who is advising or has advised the United States, with respect to a Federal agency procurement, and who by virtue of that office, employment, or relationship has had access to contractor bid or proposal information, source selection information, or award information.

Individuals shall not disclose, solicit, or obtain, directly or indirectly, any procurement requirements, Government pricing estimates, contractor bid or proposal information, proprietary information, or source selection information regarding such procurements prior to or following the contract award.

These prohibitions apply to Federal employees, contractor and subcontractor personnel, consultants, experts, and advisors. Certifications are required stating that the requirements set forth herein have not been violated. Violators will be liable for

contractual penalties and administrative actions as well as civil penalties up to \$100,000 for individuals and \$1,000,000 for corporations, and criminal penalties up to five years imprisonment.

In the spirit of the OFPP Act of 1988, as revised by the Clinger-Cohen Act of 1996, you are requested to read and certify to the following:

1. I certify that I will not disclose any government requirements, contractor proposal or award information, proprietary pricing or technical information, and/or labor hour rate information throughout the duration of the awarded contract (and six years three months after final payment, per FAR 4.804).
2. I certify that if I receive, see, or use any proprietary information of contract awards or pricing data, that I shall not disclose this proprietary information to any unauthorized person or use it for personal benefit during or after my term of employment under contract with USDA.
3. I certify that any analysis or evaluation of data that I may perform, or database or other systems that store that data and are based on the contents of contract awards that I may design or develop, will be kept confidential and I will not discuss that data with anyone outside of NITC Resource Management Division (RMD) employees, as directed.
4. I certify that this confidentiality will be maintained even after the contract has been concluded and my employment may be terminated as contract support to NITC.

I hereby certify that I have read the aforementioned; that I am familiar with the law and policies governing the disclosure of sensitive and proprietary information; and that I fully and completely observe them and will not disclose the above-mentioned information to any unauthorized person.

Name (Please Print)

Signature

(Date)



NITC Manual

Human Resources Management Contractor Exit Process



For Internal Data Center Personnel

SHORT REFERENCE

ACM-0015-02

(Revision 2)

**UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114**

**UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114**

REVIEW AND REVISION HISTORY

Review and Revision History

RELEASE DATE:	
NEXT RELEASE:	

REVIEW DATE:	REVIEWER NAME:	ACTION TAKEN:

REVISION DATE:	REVISOR NAME:	SUMMARY OF CHANGES:
08/24/11	Sue Brackney	Applying NITC Standard Template to the contractor process.
10/17/11	Sally Soule	Re-number Section 6

**UNITED STATES DEPARTMENT OF AGRICULTURE
OFFICE OF THE CHIEF INFORMATION OFFICER
NATIONAL INFORMATION TECHNOLOGY CENTER
KANSAS CITY, MO 64114**

NITC MANUAL	SERIES: ACM NUMBER: 0015 -02 REVISION:
SUBJECT: NITC Directive Management Program NITC Contractor Exit Process	EFFECTIVE DATE: August 26, 2011 LAST AMMENDMENT DATE: 10/17/11
APPROVED BY: Deputy Associate Chief Information Officer -Business, Finance & Security	OPI: Resource Management Division /Contract Management Branch AUTHOR: Phil Gehrt

AMENDMENT HISTORY

AMENDMENT DATE:	SECTION NAME / PARAGRAPH:	SUMMARY:	APPROVED BY:

NATIONAL INFORMATION TECHNOLOGY CENTER MANUAL

TABLE OF CONTENTS

Table of Contents	Page
REVIEW AND REVISION HISTORY	2
AMENDMENT HISTORY	3
TABLE OF CONTENTS.....	4
1. PURPOSES	5
2. SOURCES OF AUTHORITY AND REFERENCES	5
3. SPECIAL INSTRUCTIONS/CANCELLATIONS	5
4. POLICY.....	5
5. RESPONSIBILITIES	5
6. EXIT PROCESS RESPONSIBILITIES.....	6
APPENDIX A 1	
REPORTS AND FORMS.....	1
APPENDIX B 1	
ABBREVIATIONS	1
APPENDIX C 1	
(Page left blank for future revisions)	1
ATTACHMENTS 1-5.....	1-6

NATIONAL INFORMATION TECHNOLOGY CENTER MANUAL

1. PURPOSE

This manual describes the NITC Contractor exit process. The purpose of this Manual is to establish an overview of the exit procedure for Contract employees leaving the National Information Technology Center (NITC) through resignation, reassignment, or other types of departure actions, and to ensure that all items of government property, security access cards, keys, equipment, etc., are returned prior to departure.

2. SOURCES OF AUTHORITY AND REFERENCES

Authority for managing the Human Resources Management Contractor Exit Process and function is authorized by law and regulations, as follows:

- a. DR 3099-001, Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees.
- b. National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This manual creates the ACM-0015-02, "Contractor Employee Exit Process", Basic, dated August 26, 201.

4. POLICY

- a. This NITC Contractor Exit Process must be followed with all required forms completed in order to comply with, and satisfy, the above-mentioned authorities and references.
- b. Scope: This manual applies to all new/in-coming contract employees to NITC at the Kansas City and Ft. Collins locations. All other NITC locations are excluded at this time.

5. RESPONSIBILITIES

- a. Resource Management Division / Contract Management Branch
 - (1) Issues directives and revisions to existing directives.
 - (2) Notifies the RO when a directive is deemed obsolete.

- b. NITC Senior Staff (including Required Clearance Officials).
 - (1) Reviews and/or comments on each draft directive.
 - (2) Indicates concurrence with the draft via electronic signature, electronic initials, or voting features.
- c. Signing Authority.
 - (1) Signing authority for this process will be the DACIO for Business, Finance & Security.

6. EXIT PROCESS RESPONSIBILITIES

For Contract employees exiting from NITC, the COTR will ensure that the NITC Contract Employee Exit Process has been completed before the contract employee leaves NITC.

- a. Contractor Site Manager
 - (1) Notify COTR/COR of contract employee's departure
 - (2) Assist COTR in all aspects of the contract employee exit process
 - (3) Obtain all contract documentation deliverables from departing contract employee
- b. NITC COTR
 - (1) Initiates the exit process using the NITC Contract Employee Exit Process Checklist (Attachment 1).
 - (2) Refers the separating employee to the ACM-0015-00 Exit Procedure.
 - (3) Keeps copies of all exit forms, including the NITC System User ID Check List.
 - (4) Completes, signs and delivers the NITC System User ID Check List Form (Attachment 4) to PPSEO.
 - (5) Completes and submits the Delete a User Account Request and the Distribution List Modification/Deletion Request on the Washington Communications and Technology Services (WCTS) forms web page found at:
<http://www.wtso.usda.gov/csb/availforms.htm>.
 - (6) Completes the Employee Document/Software Removal/Non-Removal Certification (Records Management) Form (Attachment 3) by:

- (a) Obtaining the Contractor employee's signature
 - (b) Signing as the Supervisor/Reviewing Official
 - (c) Obtaining the OCIO Records Officer signature
 - (d) Returning the form to the Resource Management Division Records Officer.
- (7) Maintains a copy for their file of the Final Employee Exit Checklist (Attachment 4). Facilitates the completion of the Final Contractor Exit Checklist (Attachment 4) by:
- (a.) Obtaining Security Division signature and date for sections 2, 4 and 7:
 - i. Returned USDA Photo Identification and LinkPass Cards.
 - ii. Returned all other Identification and building access cards.
 - iii. Returned NITC Parking Tag(s)
 - iv. Verified and returned NITC System User ID Checklist (Attachment 2).
 - v. Personnel Security Debriefing completed.
 - (b.) Obtaining Resource Management Division signature and date for section 8 for return of the following equipment:
 - i. Cell phones, laptops (including property pass), air cards, GETS Card, Remote Access Tokens and serial numbers, along with any other assets such as keys, etc. (NOTE: The RMD signatory should refer to all spreadsheets to verify whether the contract employee has been issued Government Furnished Property (GFP), such as laptop, blackberry/cell phone, RSA key, GETS card, etc.. Ensure all spreadsheets are updated accordingly.)
 - ii. If any items listed on the Final Employee Exit Checklist have been identified as lost or stolen, fill out the report of Lost/Stolen Equipment Incident to Cyber Security form (Attachment 5) and forward to Cyber Security.
 - (c.) Notifies Contingency Planning group to remove contract employee name from emergency call tree system.
- c. SECURITY- PERSONNEL/PHYSICAL SECURITY AND ENGINEERING OFFICE (PPSEO)
- (1) Sends out e-mail to responsible Security staff and other functional areas involved, instructing them to remove/disable system access privileges

(2) Conducts the Employee Security Debriefing, ensuring all involved have correctly followed the details, recovered appropriate property and completed the forms contained in this exit procedure as necessary.

(3) Files the NITC System User ID Check List form (Attachment 2).

d. WCTS HELPDESK

(1) Disables user ID and renaming\archiving functions on the employee's file folder on the shared drive H:\

APPENDIX A

REPORTS AND FORMS

TABLE A1

REPORTS

NUMBER	REPORT TITLE	DESCRIPTION	SOURCE
None for this amendment.			

TABLE A2

FORMS

This Table lists all forms referenced in this handbook

NUMBER	TITLE	DISPLAY	REFERENCE
None for this amendment.			

APPENDIX B
ABBREVIATIONS

TABLE B1

Abbreviation	DEFINITION
BF&S	Business, Finance & Security
CMB	Contract Management Branch
COTR	Contracting Officer's Technical Representative
COR	Contracting Officer's Representative
LAN	Local Area Network
NEIS	Non-Employee Information System
NITC	National Information Technology Center
PPSEO	Personnel/Physical Security & Engineering Office
RMD	Resource Management Division
WCTS	Washington Communications and Technology Services

APPENDIX C

(Page left blank for future revisions)

ATTACHMENT 1



Office of the Chief Information Officer


NITC Contractor Employee Exit Process Checklist

AREAS	ITEMS	RESOURCES
COTR WILL ENSURE ALL FORMS ARE COMPLETE BEFORE SEPARATION.		
COTR	<ul style="list-style-type: none"><input type="checkbox"/> NITC Contract Employee Exit Process Checklist (this checklist), Attachment 1<input type="checkbox"/> NITC System User ID Check List, Attachment 2<input type="checkbox"/> Employee Document Removal/Non-Removal Certification, Attachment 3<input type="checkbox"/> Final Employee Exit Checklist, Attachment 4<input type="checkbox"/> Report of Lost/Stolen Equipment Incident to Cyber Security, Attachment 5	W:CENTER\DIRECTIVE-ADMIN\Current\ACM 002 – Employee Exit Process Directive

ATTACHMENT 2

EMPLOYEE DOCUMENT REMOVAL/NON-REMOVAL CERTIFICATION

NITC SYSTEM USER ID CHECK LIST

 employee/contractor

(name)

System Name	Userid's		System Name	Userid's	
Mainframes			Software Products		
USDA			Teleview		
Production					
FFIS			TPX		
EASE			Omegamon		
NFC/Other			Netview		
Network			Servers		
OALAN					
Routers/Switches					
TACACS					
SecureRemote					
Monitors					
Firewall					
IDS					
RSA Token S.N.					
Applications			Other		
CICS					
Database					
Sametime/QP					
Avue			eAUTH:Applications		
			CSAM		
			GovTrip		
Vendor Support			Aglearn		
CA Star-TCC			WebTA		
IBM Link			Etc:		

This form will be completed by the employee/contractor prior to exiting.

This form will be completed and signed by the losing and gaining supervisors for those federal employees transferring to other divisions within NITC. The Security Office will retain this form.

Losing Supervisor

Date

Gaining Supervisor

Date

ATTACHMENT 3

EMPLOYEE DOCUMENT/SOFTWARE REMOVAL/NON-REMOVAL CERTIFICATION

Name _____

Office _____

Supervisor _____

Are you removing any official documents/software from the National Information Technology Center (NITC) upon your departure?

YES If yes, continue

NO If no, see below

Reason for Removal:

I certify that the document(s)/software that I am removing from the NITC have been reviewed and approved for removal. A list of the documents that I have removed is attached. The document(s)/software that I am removing do not include program information that, if released, would impair the operations of the National Information Technology Center.

Signature of Employee

Date

Reviewing Official:

Signature of Reviewing Official

Date

By my signature, I certify that I am NOT removing any documentation/software from the NITC.

Signature of Exiting Employee

Date

Received:

OCIO Records Officer

Date

Criminal penalties are provided for the unlawful removal or destruction of official records (18 U.S.C. 207)

ATTACHMENT 4

FINAL CONTRACT EMPLOYEE EXIT CHECKLIST

FINAL EMPLOYEE EXIT CHECKLIST Administrative Offset Procedures permit holding final paycheck and/or leave until accountable documents are returned.		EMPLOYEE NAME <div style="background-color: #cccccc; width: 100px; height: 15px; margin: 5px 0;"></div>	
		SEPARATION DATE (LAST DAY OF PAY STATUS) <div style="background-color: #cccccc; width: 100px; height: 15px; margin: 5px 0;"></div>	
AGENCY USDA		ORGANIZATIONAL UNIT National Information Technology Center	
ITEMS REQUIRING CLEARANCE PRIOR TO FINAL SALARY PAYMENT			
1. TRANSPORTATION REQUESTS <div style="text-align: center;">N/A</div>		8. PROPERTY (Resource Management Staff) <input type="checkbox"/> a. CELL PHONE/BLACKBERRY <input type="checkbox"/> b. LAPTOP (Including Property Pass) <input type="checkbox"/> c. AIR CARD <input type="checkbox"/> d. GETS Card <input type="checkbox"/> e. Remote Access Token _____ serial # <input type="checkbox"/> f. OTHER (keys, etc)	
2. IDENTIFICATION CARDS (Security Staff) <input type="checkbox"/> a. USDA IDENTIFICATION (AD-53) N/A <input type="checkbox"/> b. OFM/NFC USER ID N/A <input type="checkbox"/> c. LINKPASS CARD <input type="checkbox"/> d. OTHER (SPECIFY) <div style="background-color: #cccccc; width: 100px; height: 15px; margin: 5px 0;"></div> Building Access Card		9. FUNDS (Resource Management Division) <input type="checkbox"/> a. TRAVEL ADVANCE <input type="checkbox"/> b. FIELD PARTY ADVANCE <input type="checkbox"/> c. IMPREST FUND ADVANCE N/A <input type="checkbox"/> d. COLLECTION OFFICER RECEIPTS <input type="checkbox"/> e. LEAVE AUDIT/AD-581	
3. GOVERNMENT BILLS OF LADING <div style="text-align: center;">N/A</div>			
4. PARKING PERMIT <div style="text-align: center;">NITC Parking Tag</div>			
5. DRIVER'S LICENSE (GOVERNMENT) <div style="background-color: #cccccc; width: 100px; height: 15px; margin: 5px 0;"></div>		10. GAO EXCEPTION <div style="text-align: center;">N/A</div>	
6. CREDIT CARDS (Resource Management Division) <input type="checkbox"/> a. GASOLINE <input type="checkbox"/> b. TELEPHONE <input type="checkbox"/> c. VISA-TRAVEL <input type="checkbox"/> d. VISA-PURCHASING PCMS <input type="checkbox"/> f. Other (specify)		11. FISCAL LIABILITY <div style="text-align: center;">N/A</div>	
7. OTHER ACCOUNTABLE DOCUMENTS (SPECIFY) <input type="checkbox"/> a. NITC SYSTEM USER ID CHECK LIST <input type="checkbox"/> b. PERSONNEL SECURITY DEBRIEFING		12. SERVICE AGREEMENTS FULFILLED <input type="checkbox"/> a. TRANSFER OF OFFICIAL STATION <input type="checkbox"/> b. FIRST POST OF DUTY <input type="checkbox"/> c. TRAINING	
		13. OTHER INDEBTEDNESS <input type="checkbox"/> a. ADVANCED S/L <input type="checkbox"/> b. ADVANCED A/L <input type="checkbox"/> c. ADVANCED COMP <input type="checkbox"/> d. LEAVE AUDIT	
REMARKS: LEAVE BALANCES A/L <div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div> S/L <div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div> COMP TIME <div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div> CREDIT TIME <div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div> RECORDS MANAGEMENT FORM _____			
CERTIFICATION: I certify that the identified items have been checked against official records, except as noted, the above-named employee has properly accounted for each item. Action has been taken to revoke existing delegations of authority and any assignment under the Department's position schedule bond.			
ITEMS BEING CERTIFIED <i>(List by No. Below)</i>	SIGNATURE AND TITLE OF OFFICIAL MAKING CERTIFICATION		DATE
2, 4, 7	<div style="background-color: #cccccc; width: 100px; height: 30px; display: inline-block;"></div> Security		<div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div>
6, 8, 9, 12	<div style="background-color: #cccccc; width: 100px; height: 30px; display: inline-block;"></div> Resource Management Division		<div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div>
13	<div style="background-color: #cccccc; width: 100px; height: 30px; display: inline-block;"></div> Supervisor		<div style="background-color: #cccccc; width: 50px; height: 15px; display: inline-block;"></div>

ATTACHMENT 5

REPORT OF LOST/STOLEN EQUIPMENT INCIDENT TO CYBER SECURITY

May. 3. 2007 3:07PM



No. 1664 P. 1

2A 07-016
FC: 9600-Policy
OACM-
Agave 5/2/07

United States
Department of
Agriculture

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

MEMORANDUM FOR BOYD RUTHERFORD, ASSISTANT SECRETARY FOR ADMINISTRATION

FROM: Patricia E. Healy *[Signature]*
Deputy Chief Financial Officer

APR 27 2007

Jerry Williams *[Signature]*
Deputy Chief Information Officer

APR 27 2007

SUBJECT: Policies and Procedures for Employee Separation

In the first quarter of this fiscal year, we established and serve as co-chairs of an Executive Steering Committee (ESC) to address the Information Technology (IT) Weaknesses in the Department. This ESC is a subgroup of the larger effort to address Department-wide internal control weaknesses and compliance with OMB Circular A-123. The ESC was tasked to address the IT material weaknesses identified in recent Office of Inspector General audits and the FY 2006 Federal Information Security Management Act and Office of Management and Budget Circular A-123 reviews. We have reviewed and analyzed the Department's information technology internal control weaknesses and are working with Departmental offices and the agencies to take corrective actions to remediate existing weaknesses by the end of the third quarter of this fiscal year. The ESC has determined that several of the weaknesses result from the inconsistent or lack of Department-wide policies and use of standard procedures.

In our review of logical and physical access controls for automated information systems, it came to the ESC's attention that we have a weakness in the area of employee separation. We have been unable to locate or identify Department-wide policies or standard procedures for employee separation. This weakness results in security and financial risk to the Department. It is necessary to have standard policies and procedures for employee separation to ensure that separating employees have Department-wide: returned all government assets that have access to USDA systems (personal computers, laptops, Blackberries, etc.); had logon access to USDA and other government systems and applications terminated; returned keys, badges or other physical access devices; and paid all money owed to the government prior to their departure.

If there are Department-wide policies and procedures governing employee separation, we would appreciate it if you could provide these to us as soon as possible, but no later than May 11, 2007, so we can include them in the FY 2007 A-123 review process. Copies should be sent to Annie Walker-Bradley in the Office of the Chief Financial Officer.

Thank you for your assistance with this request. If you require further information, please let us know. Patricia Healy can be reached at 202-720-0727; Jerry Williams can be reached at 202-720-8833.

AN EQUAL OPPORTUNITY EMPLOYER

Item	Description
Date and time Incident was called in to SNCC:	
Approximate date and time of the incident including the Time Zone:	
Name and Email Address of the person who is reporting this incident to SNCC:	
Telephone number of the person who is reporting this incident:	
What USDA Agency does the person work for who lost the equipment?	
Did the computer contain Personal Identity Information, proprietary, financial, or Privacy Act data?	<input type="checkbox"/> Yes (Contact CS by telephone immediately) <input type="checkbox"/> No (Send email to cyber.incidents@usda.gov) <input type="checkbox"/> Unknown (Contact CS by telephone immediately)
Was the hardware using encryption?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Unknown
Address where the Incident occurred:	[City & State]
SNCC tracking number:	
Name of SNCC reporting person:	
How did you notify Cyber Security?	<input type="checkbox"/> sent email to cyber.incidents@usda.gov <input type="checkbox"/> Called 1-866-905-6890 <input type="checkbox"/> Called Gail Phillips at 616-516-3864 <div style="text-align: right;">816-914-0312 (personal cell)</div> <input type="checkbox"/> Called Bryce Eckland at 913-438-1047 (home) <div style="text-align: right;">913-961-2448 (personal cell)</div> <div style="text-align: right;">202-320-0115 (work cell)</div>
Type and Number of Equipment lost?	